

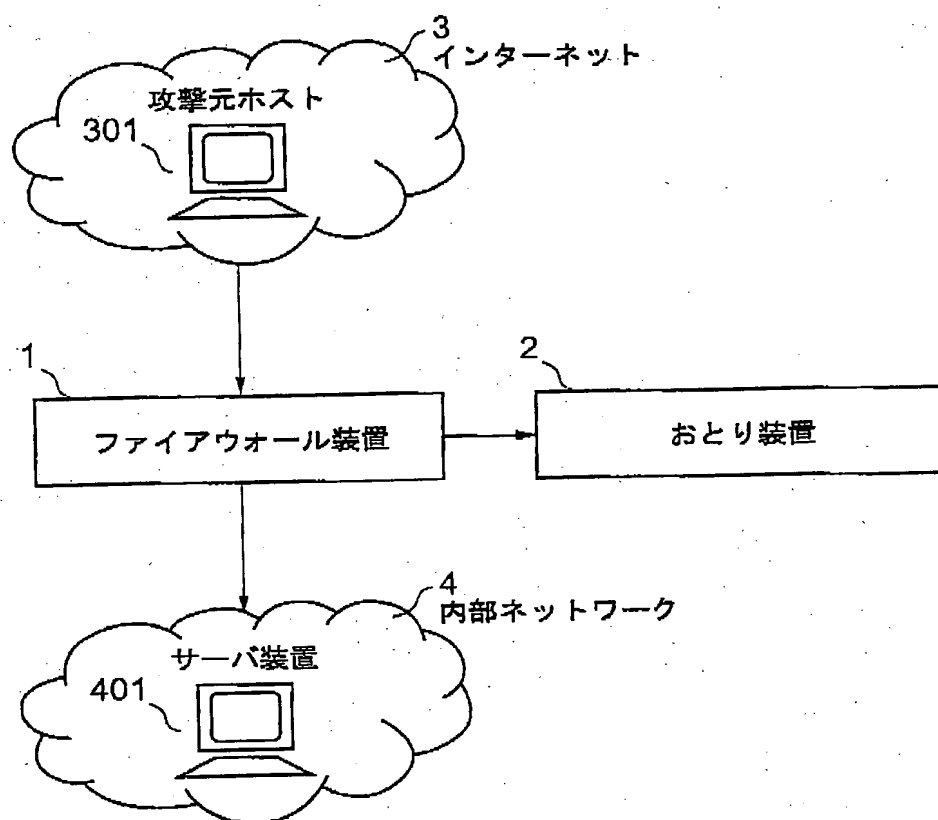
FQ 5-613 0537  
~~0518~~

整理番号 0489

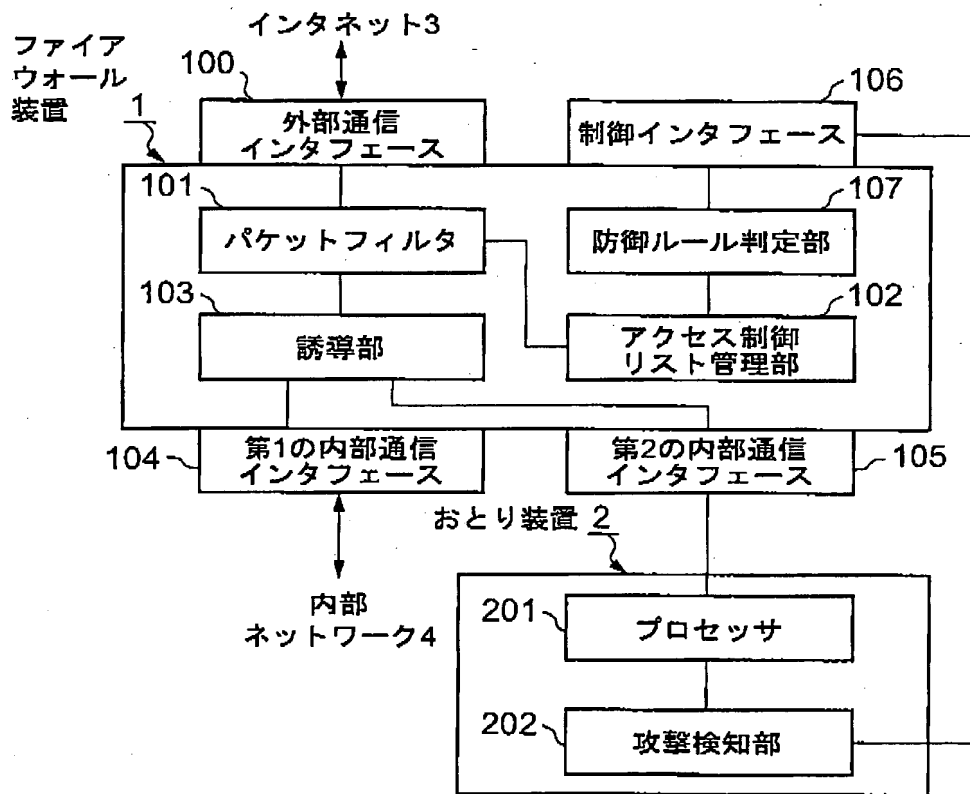
155  
(1/31)

【書類名】 図面

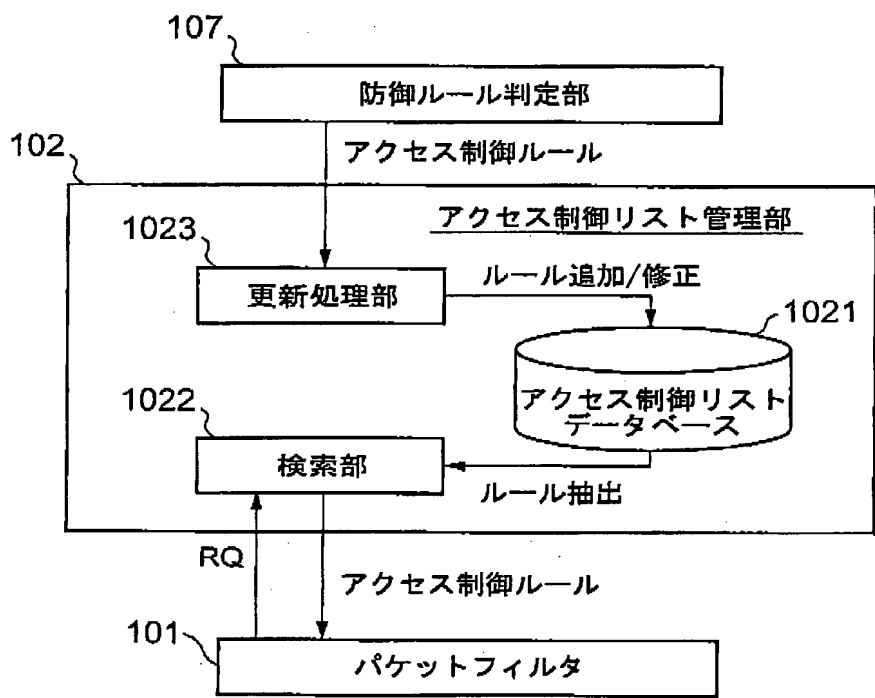
【図 1】



【図 2】



【図 3】



【図 4】

1021

アクセス制御リストデータベース		
ソースIPアドレス (SRC)	ディスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

…任意のアドレスにマッチ

ACCEPT…パケットの受理

DENY…パケットの拒否(ICMPエラーを通知)

DROP…パケットの廃棄(ICMPエラーを通知しない)

【図 5】

誘導リスト

1.2.3.1
1.2.3.2
1.2.3.3
1.2.3.5
1.2.3.6
⋮

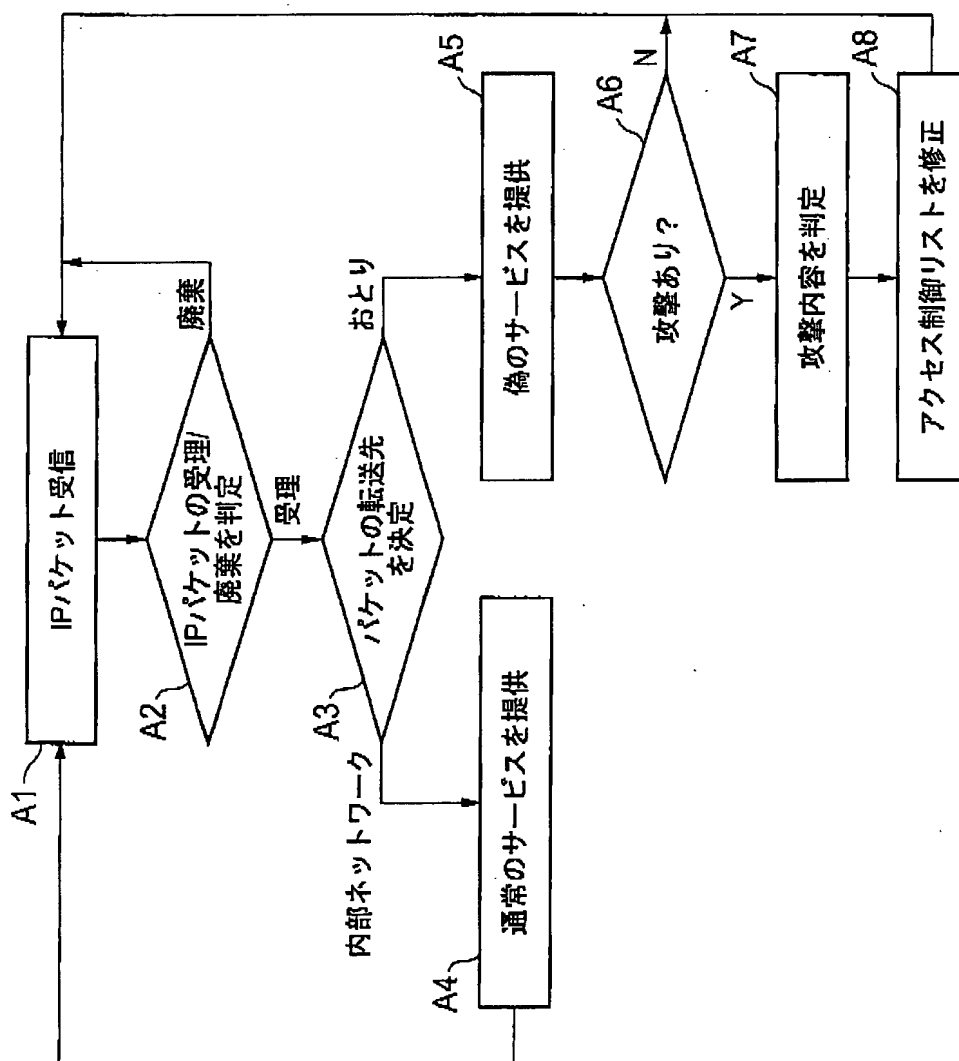
【図 6】

107

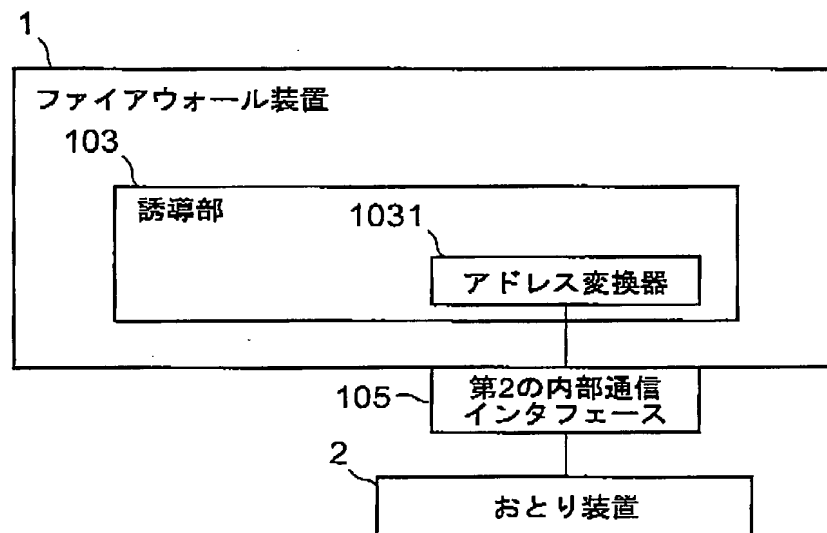
防御ルール判定部			
攻撃種別	ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
RECON	—	—	—
INTRUSION	\$(SRC_IP_ADDRESS)	*	DROP
DESTRUCTION	\$(SRC_IP_ADDRESS)	*	DROP

—…無指定(何もしない)  
\$0…置換用変数

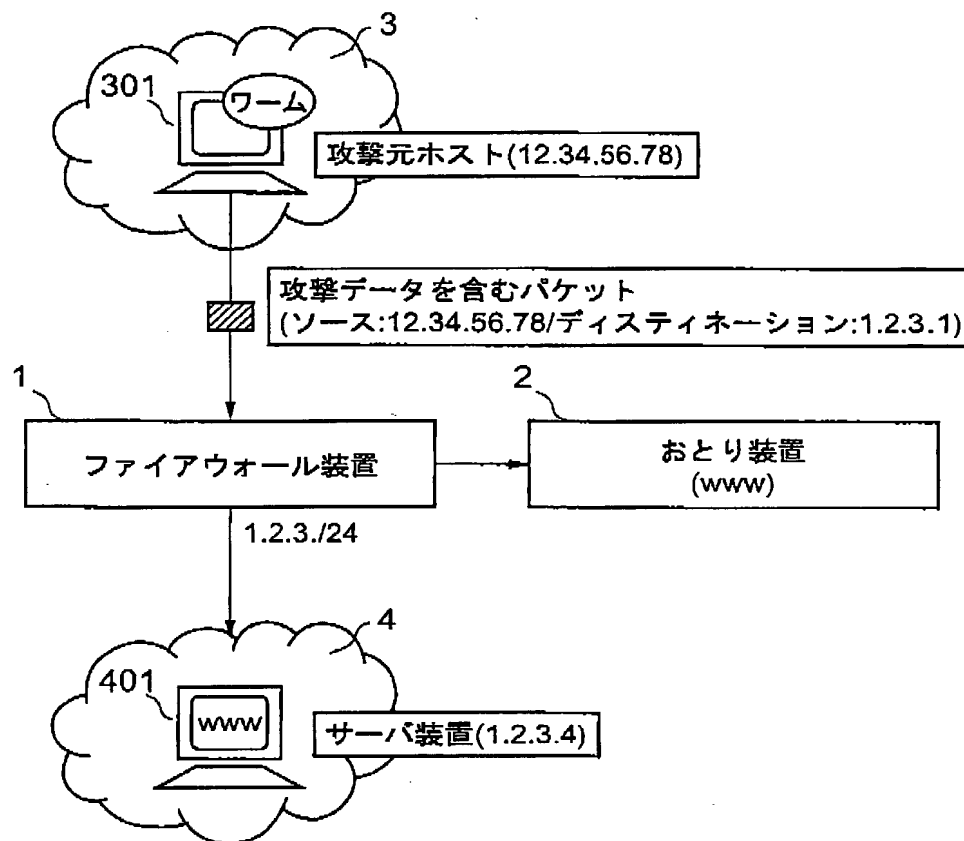
【図 7】



【図 8】

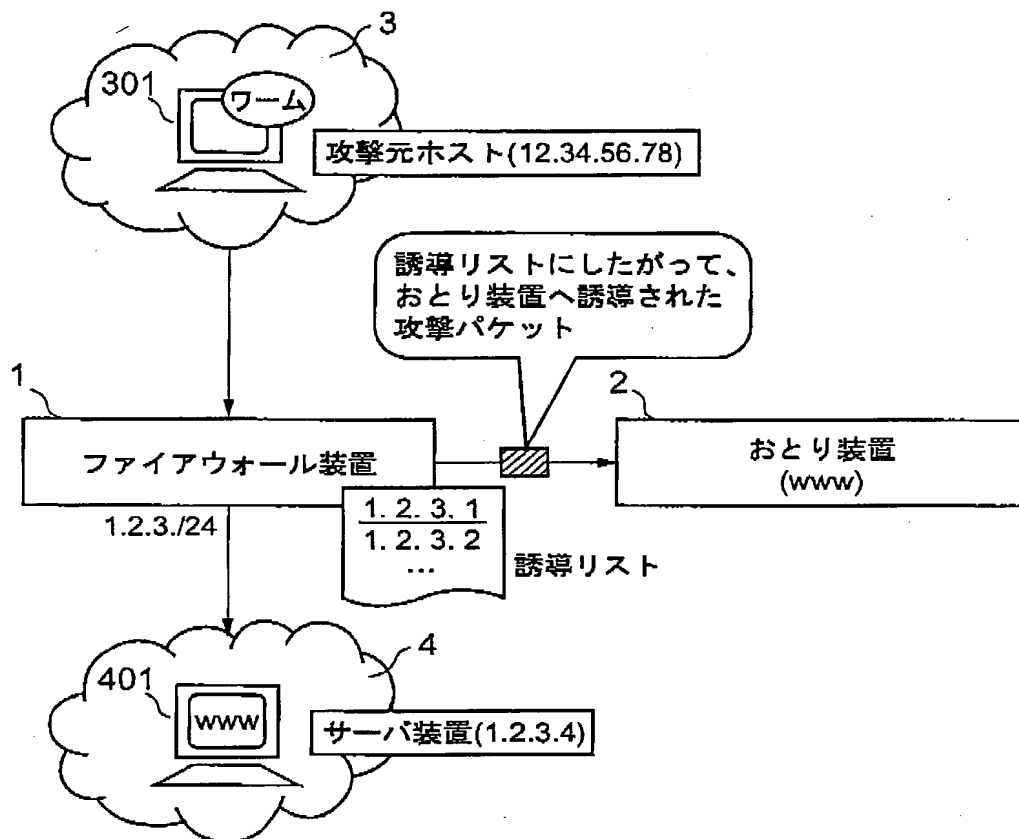


【図 9】

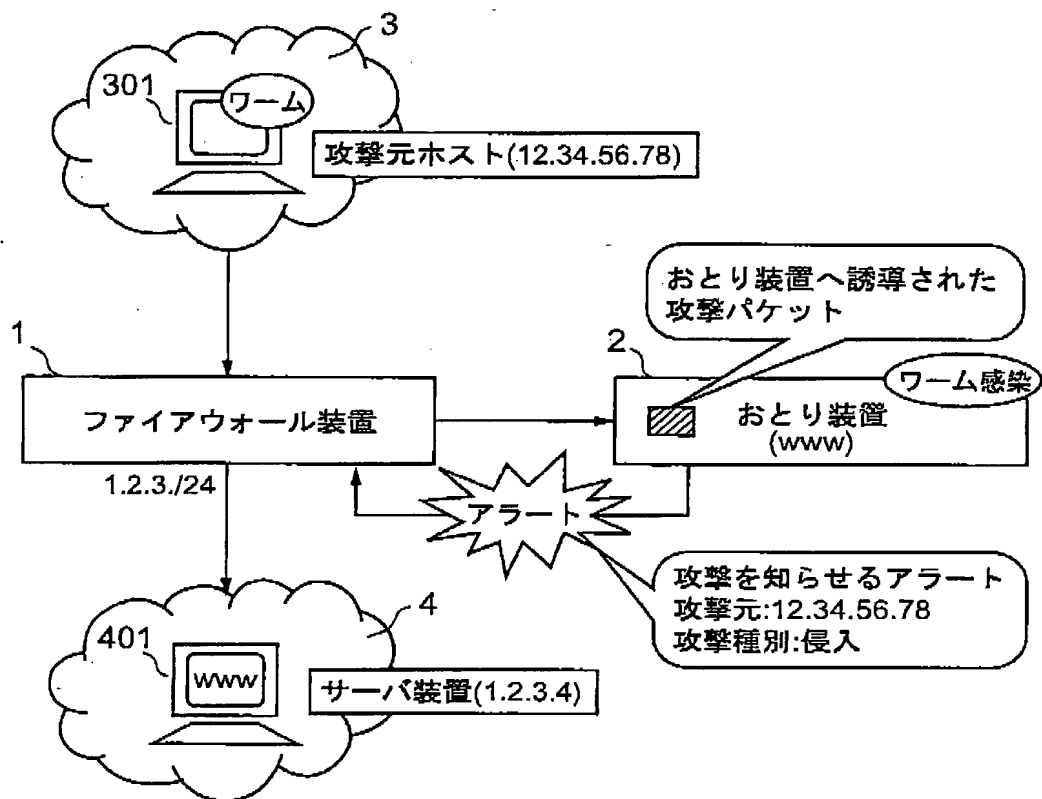




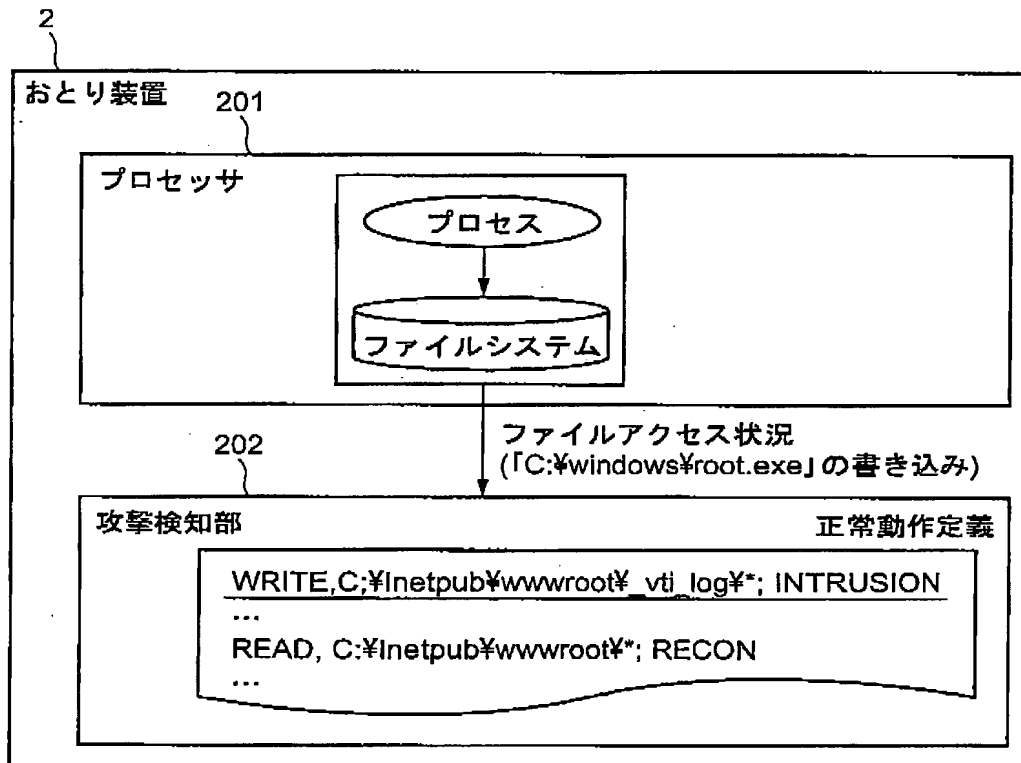
【図10】



【図11】



【図12】



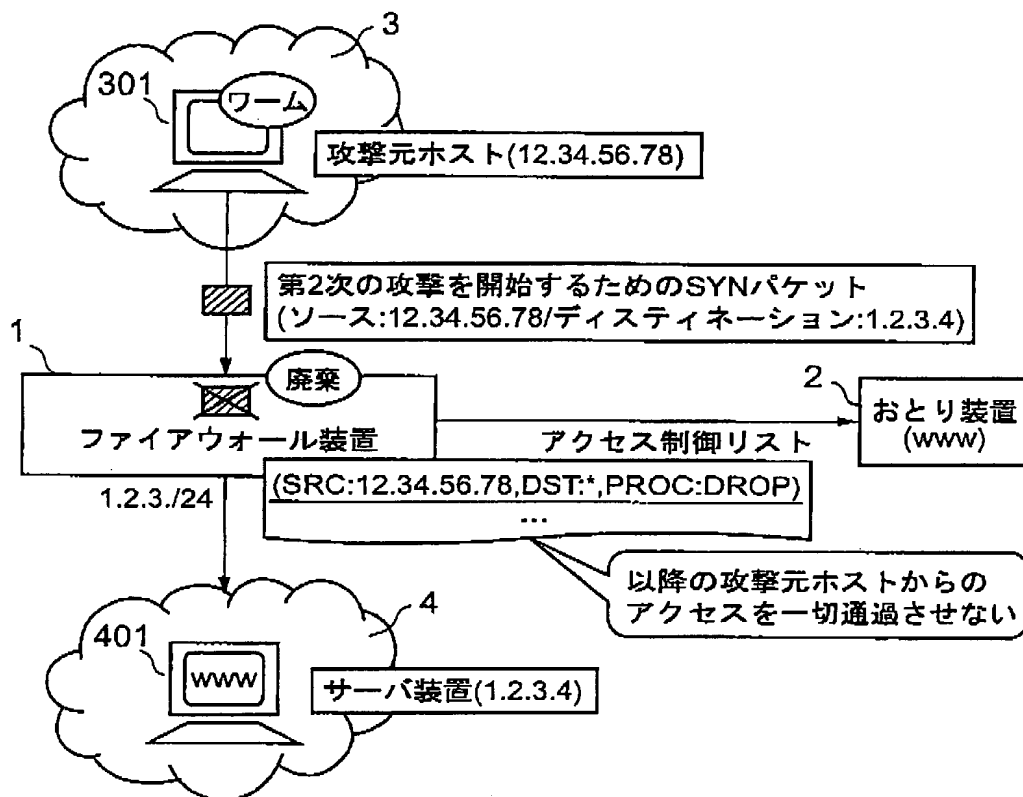
【図13】

アクセス制御リストの更新

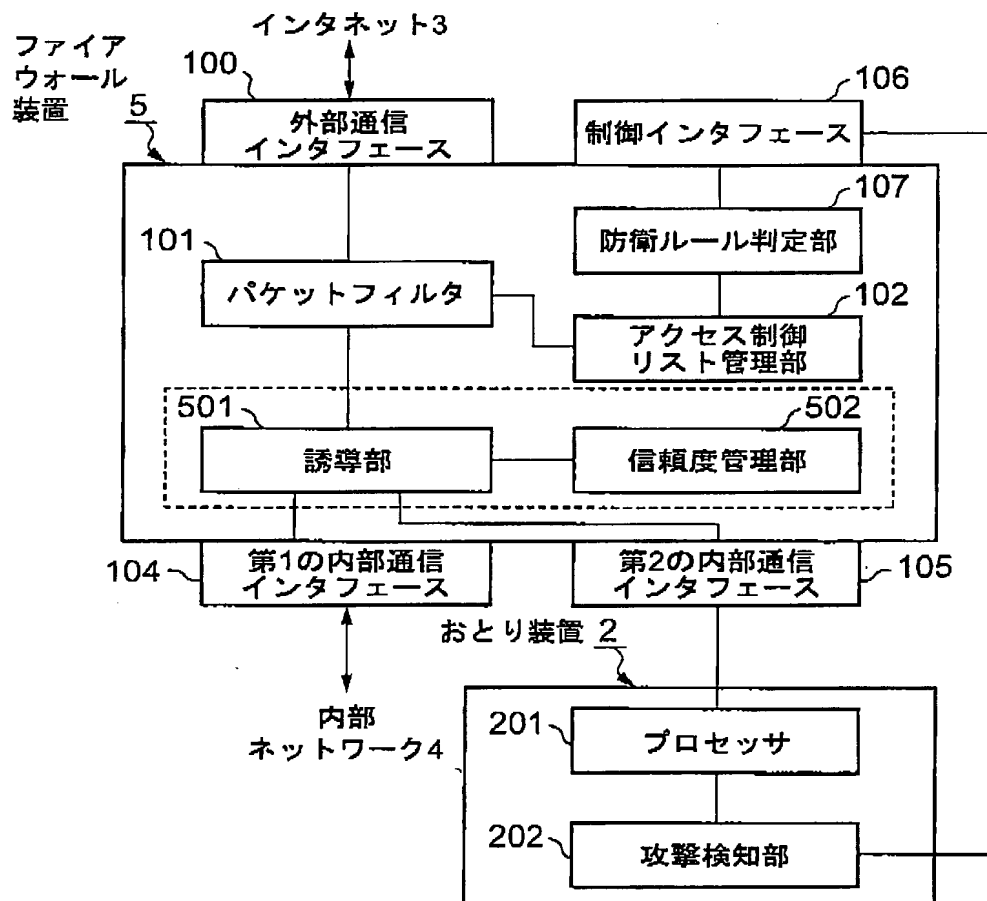
ソースIPアドレス (SRC)	デスティネーション IPアドレス(DST)	パケットフィルタ処理 (PROC)
12.34.56.78	*	DROP
*	1.2.3.1	ACCEPT
*	1.2.3.2	ACCEPT
12.34.1.1	*	ACCEPT
*	1.2.3.3	DROP
*	*	DENY

追加

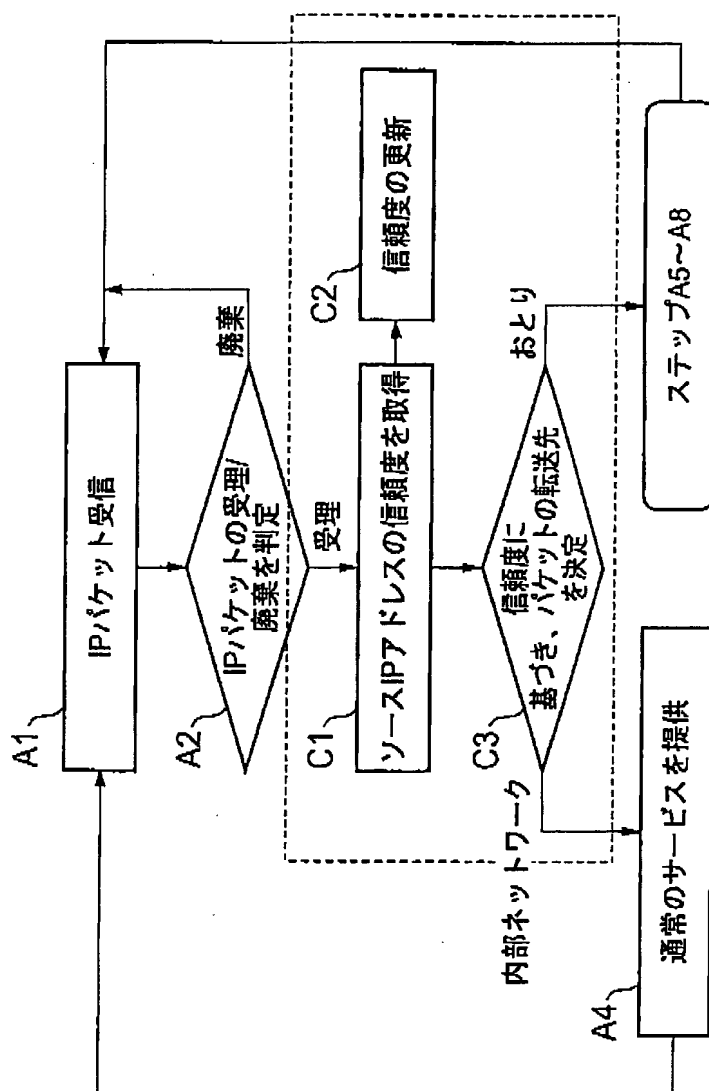
【図14】



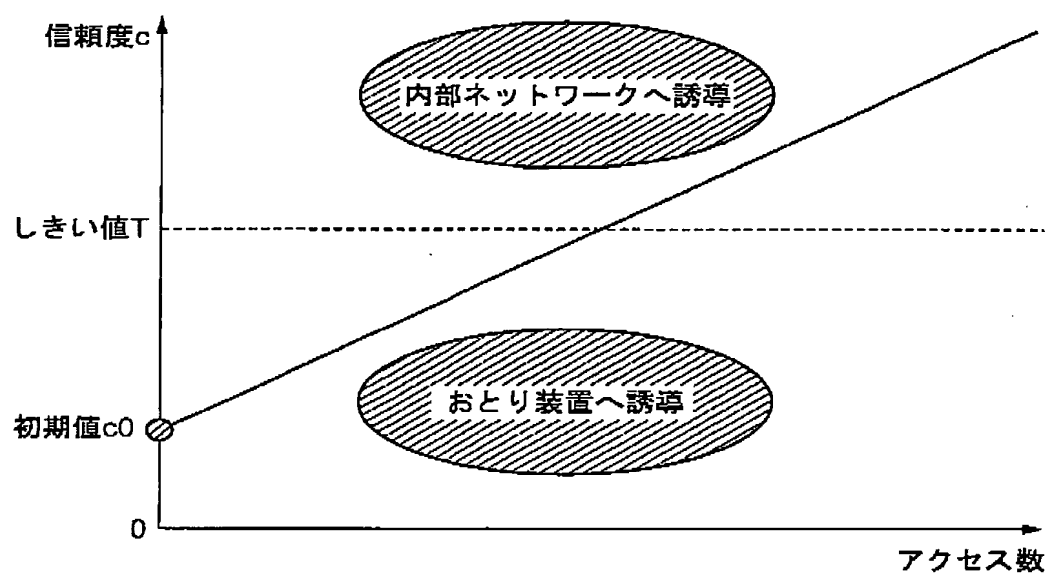
【図15】



【図16】

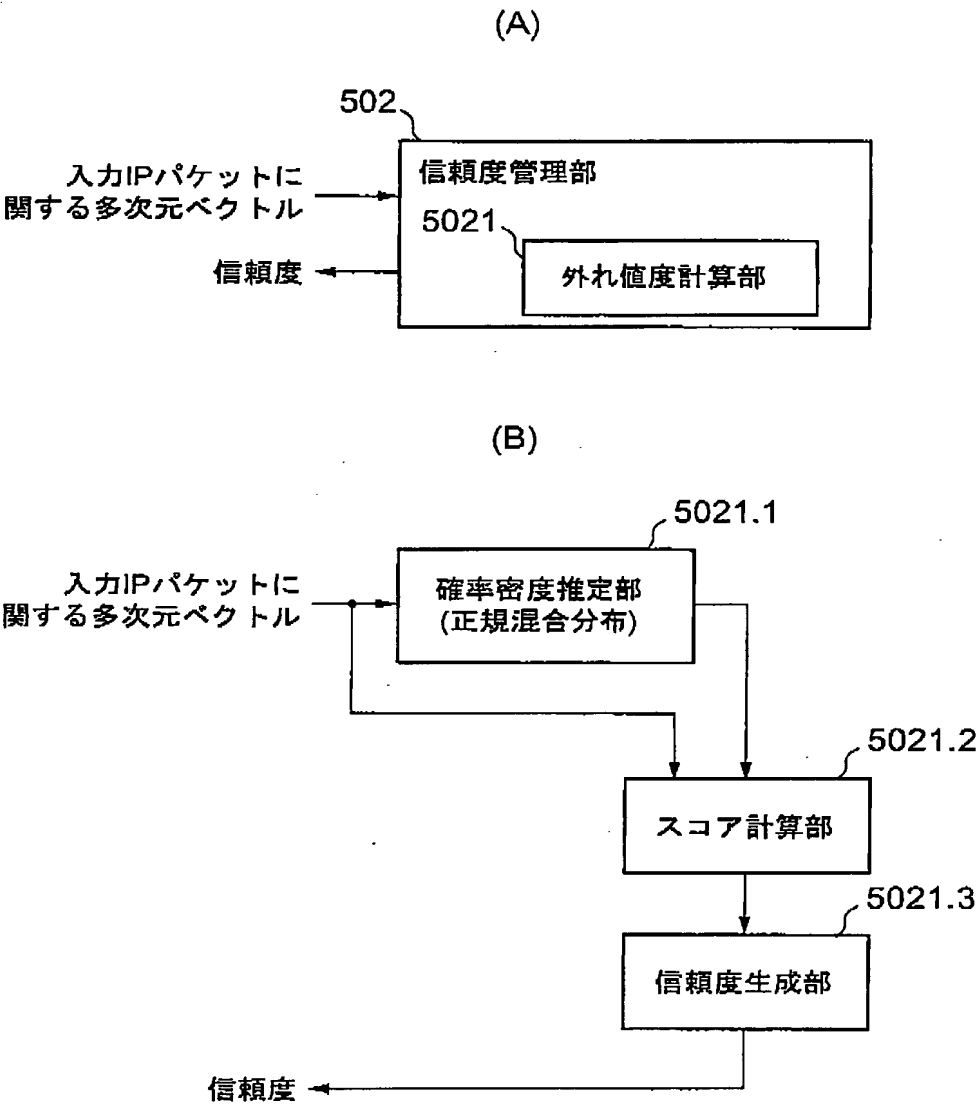


【図17】

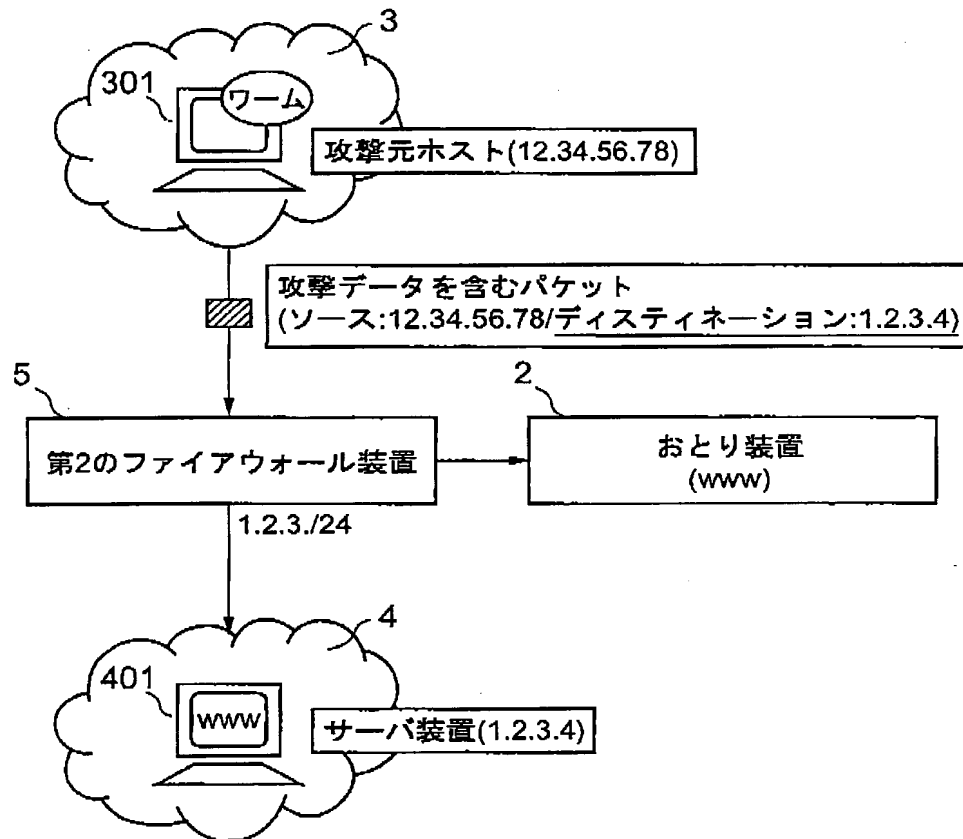




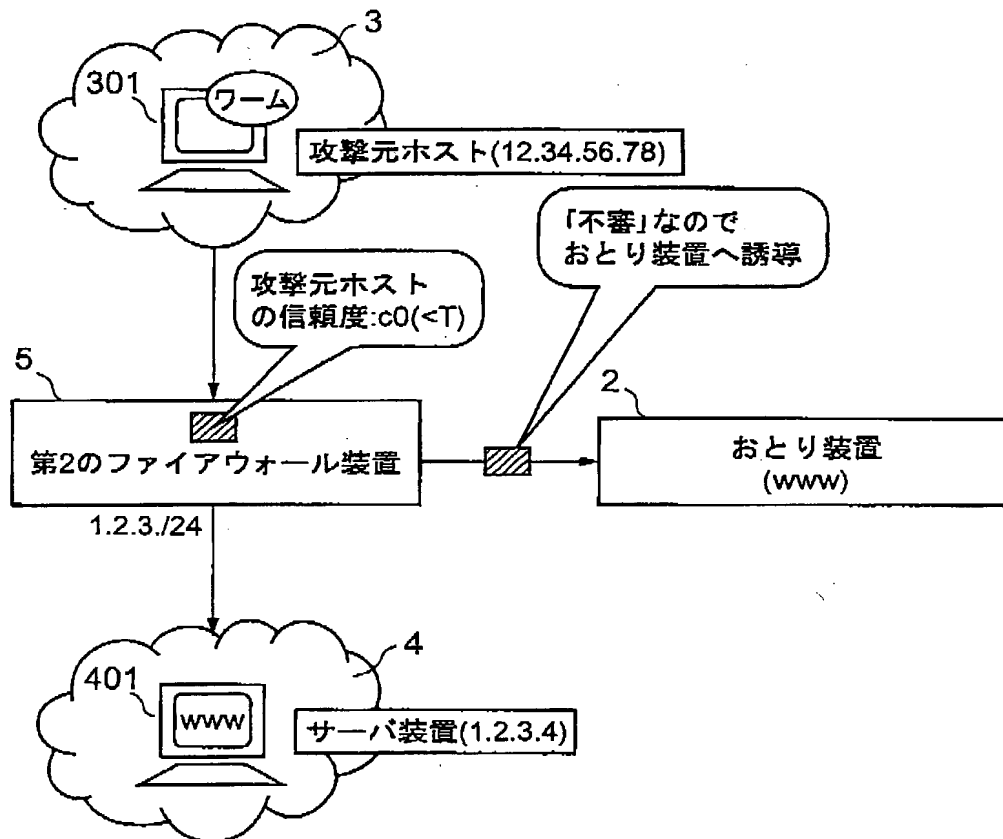
【図18】



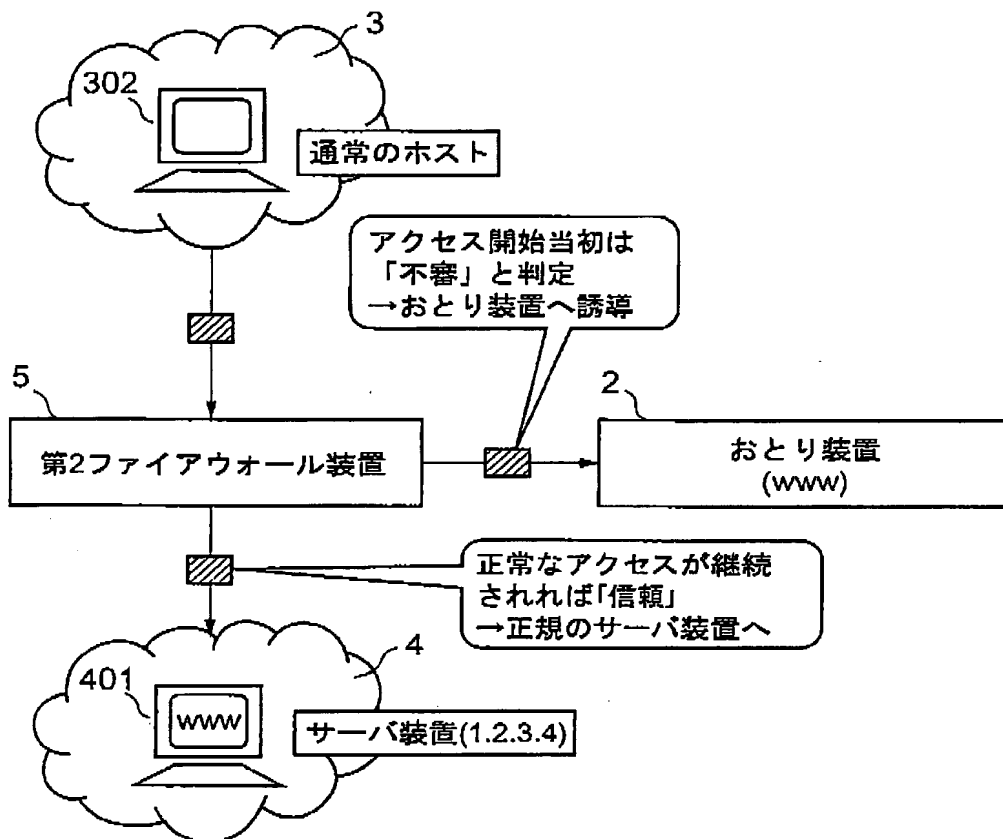
【図19】



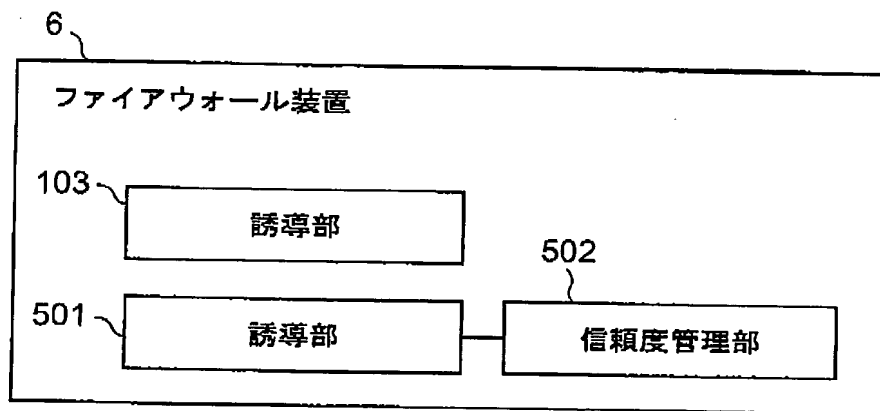
【図20】



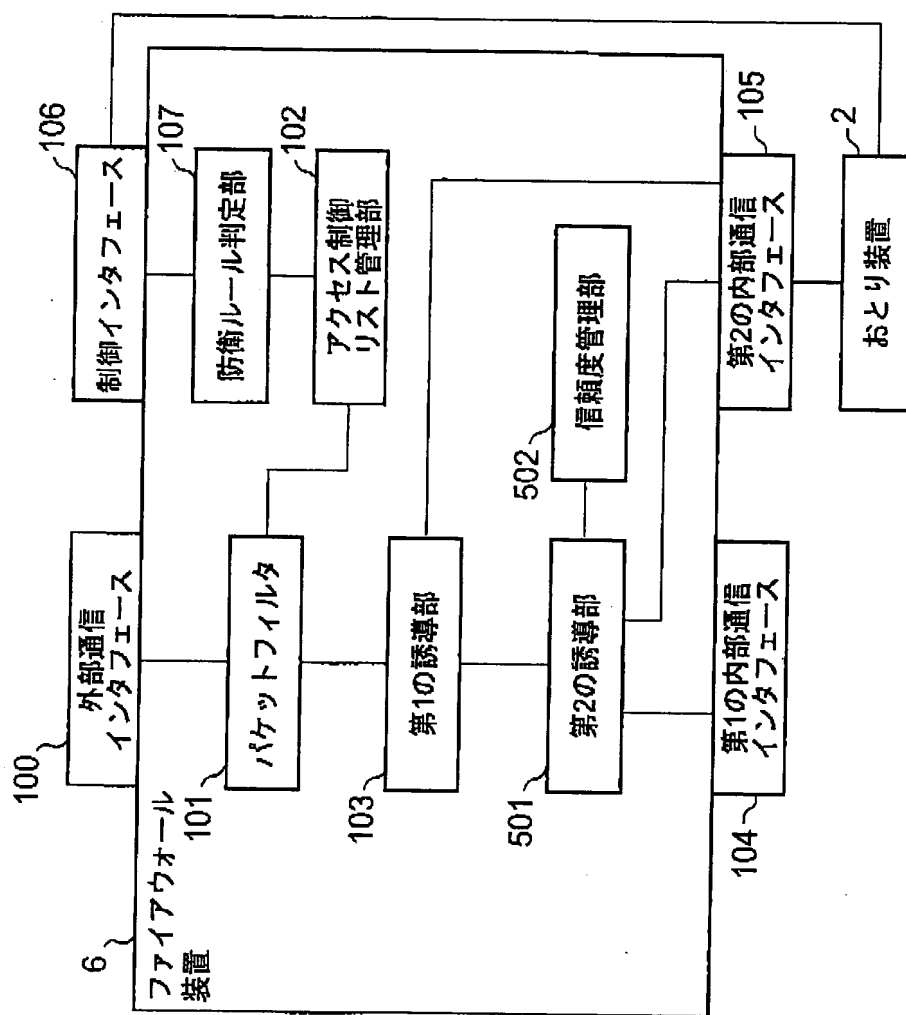
【図21】



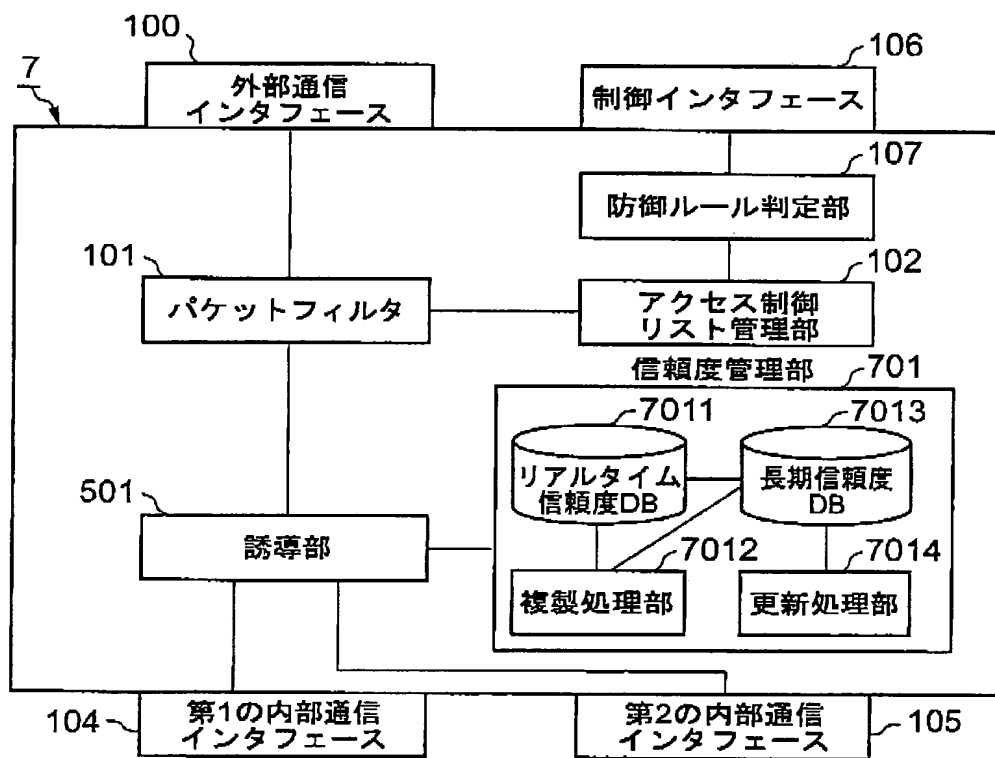
【図22】



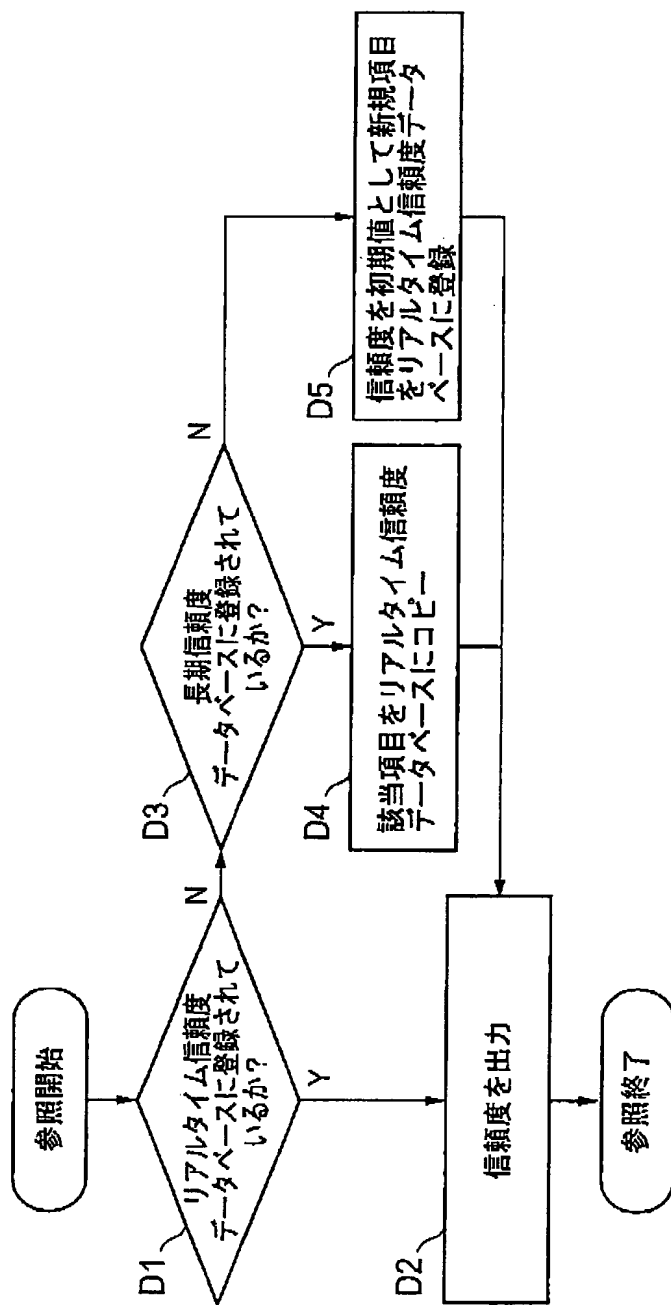
【図23】



【図24】

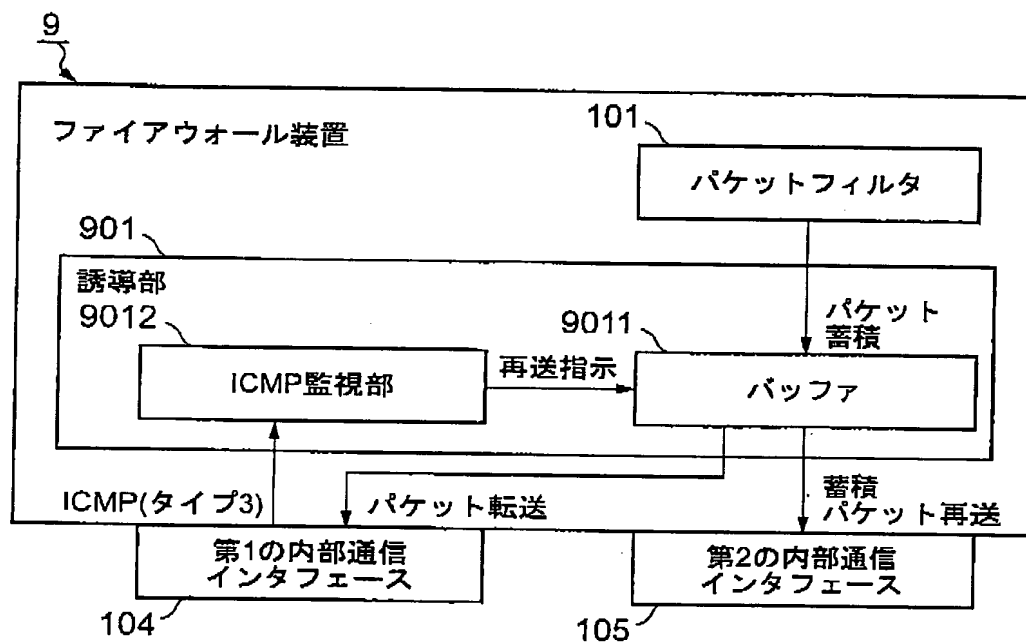


【図25】

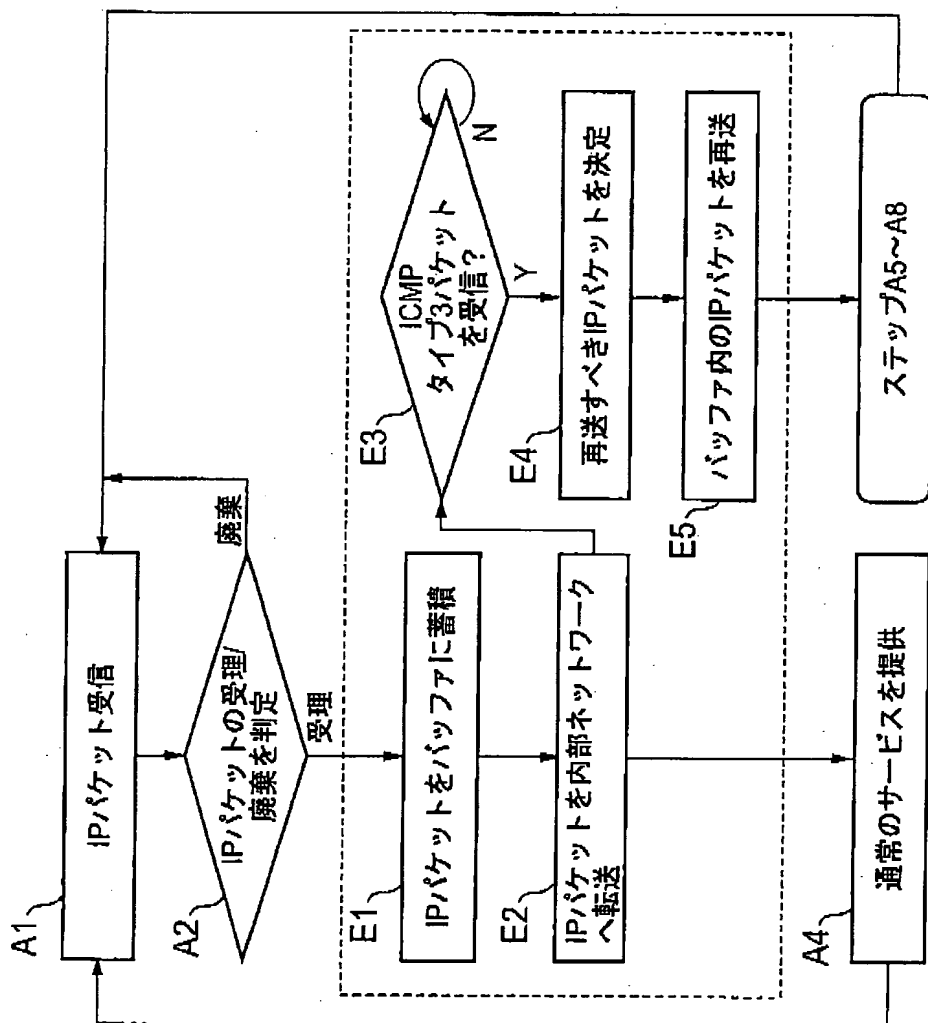




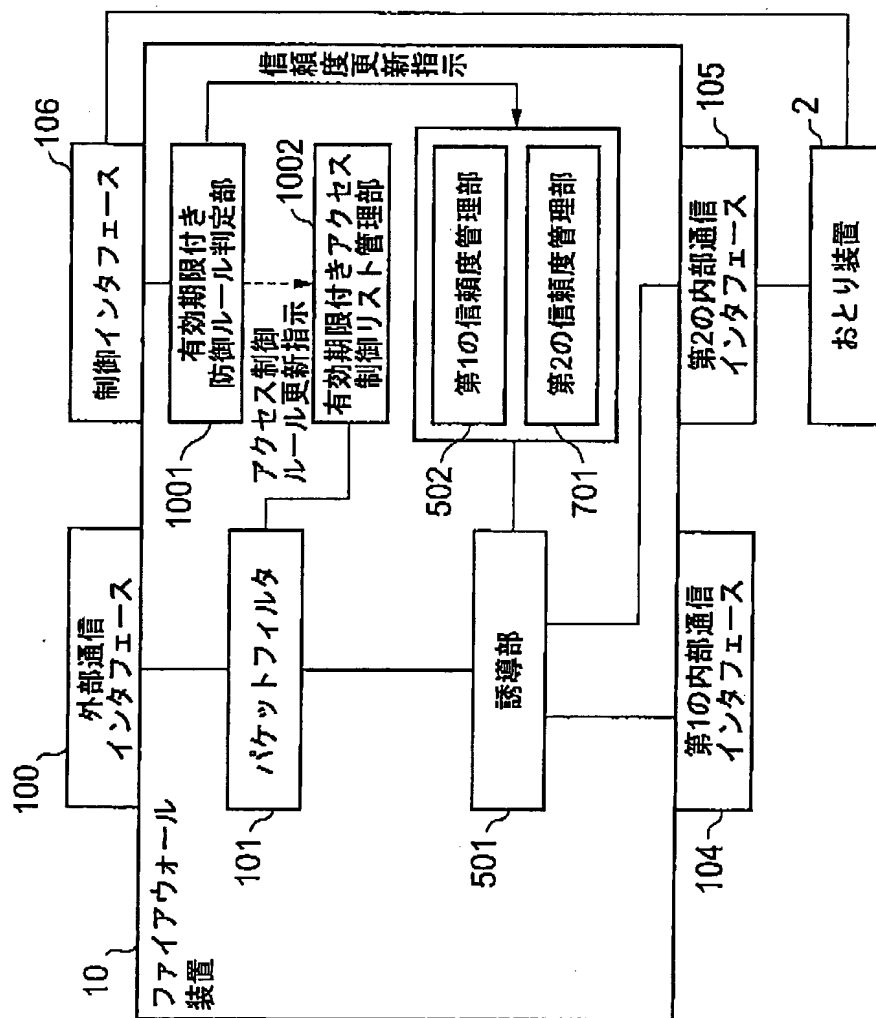
【図26】



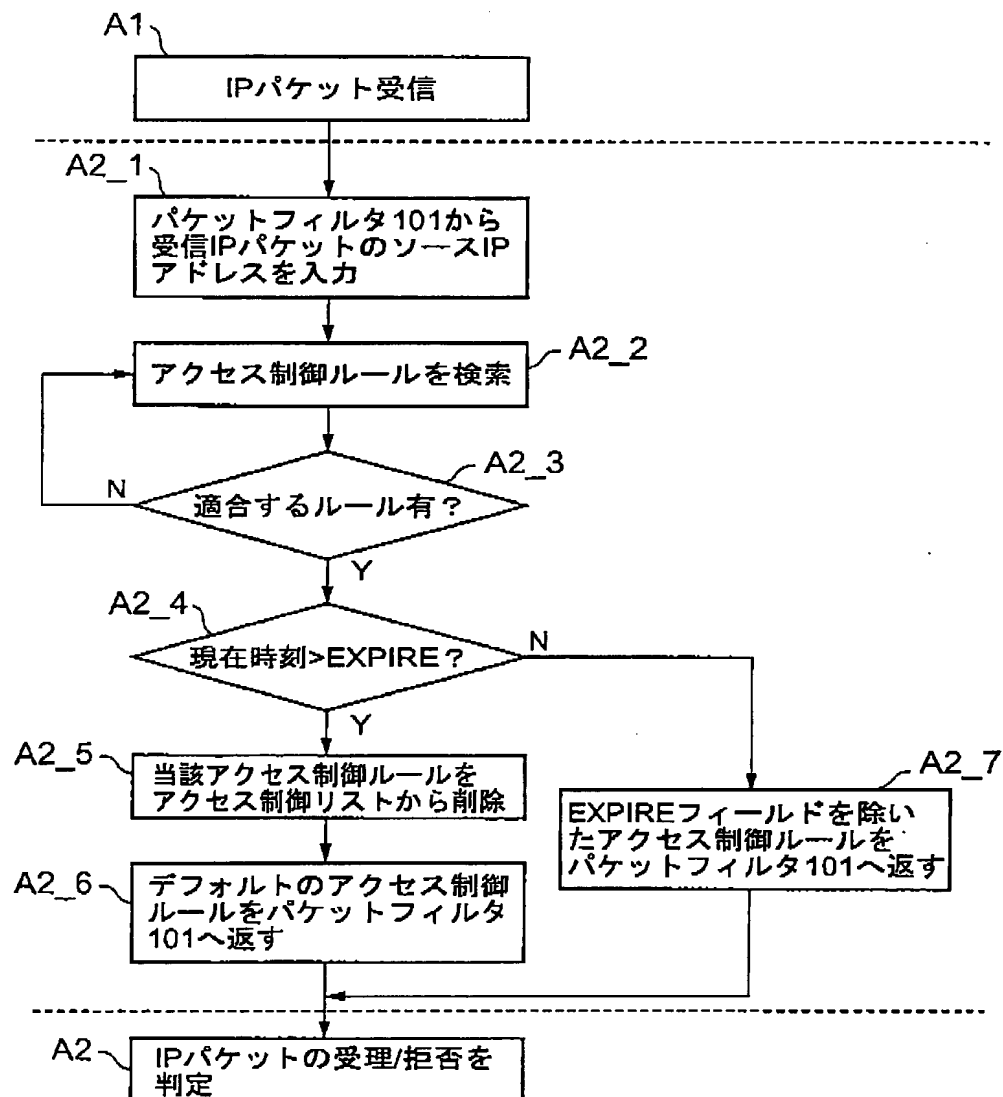
【図27】



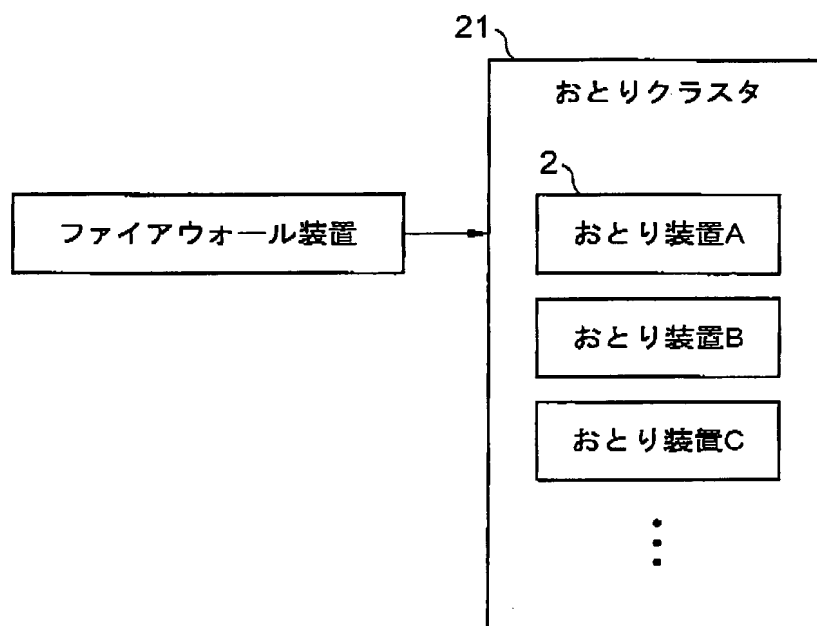
【図28】



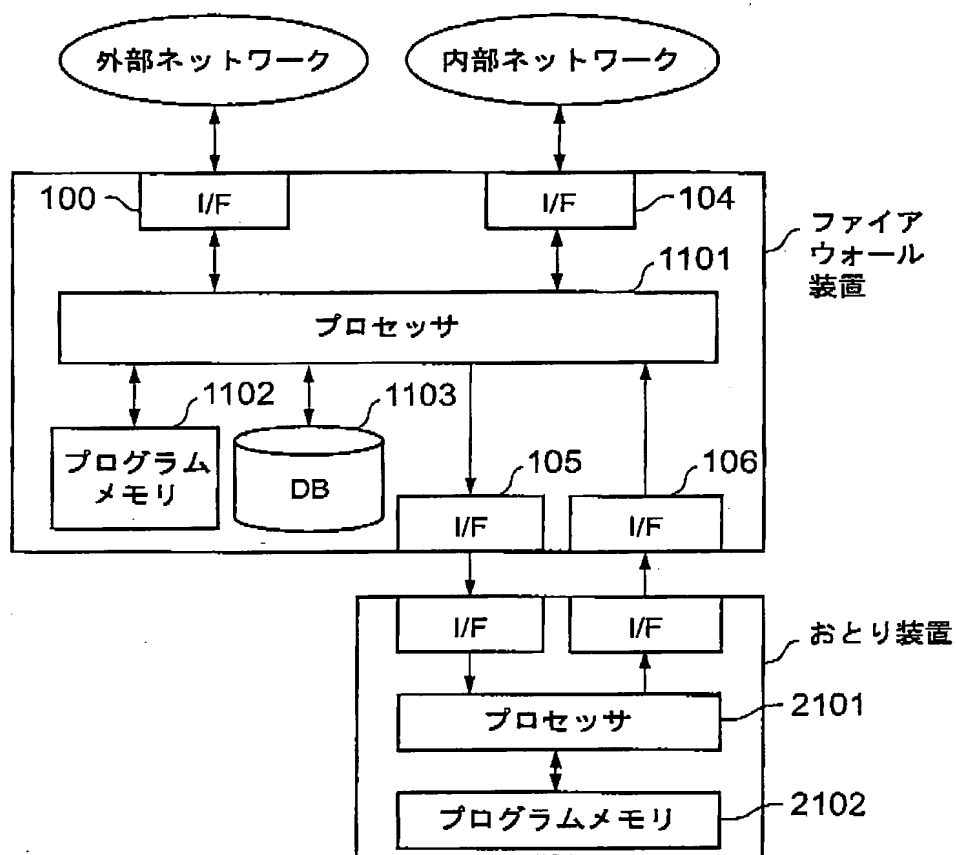
【図29】



【図30】



【図31】



【図32】

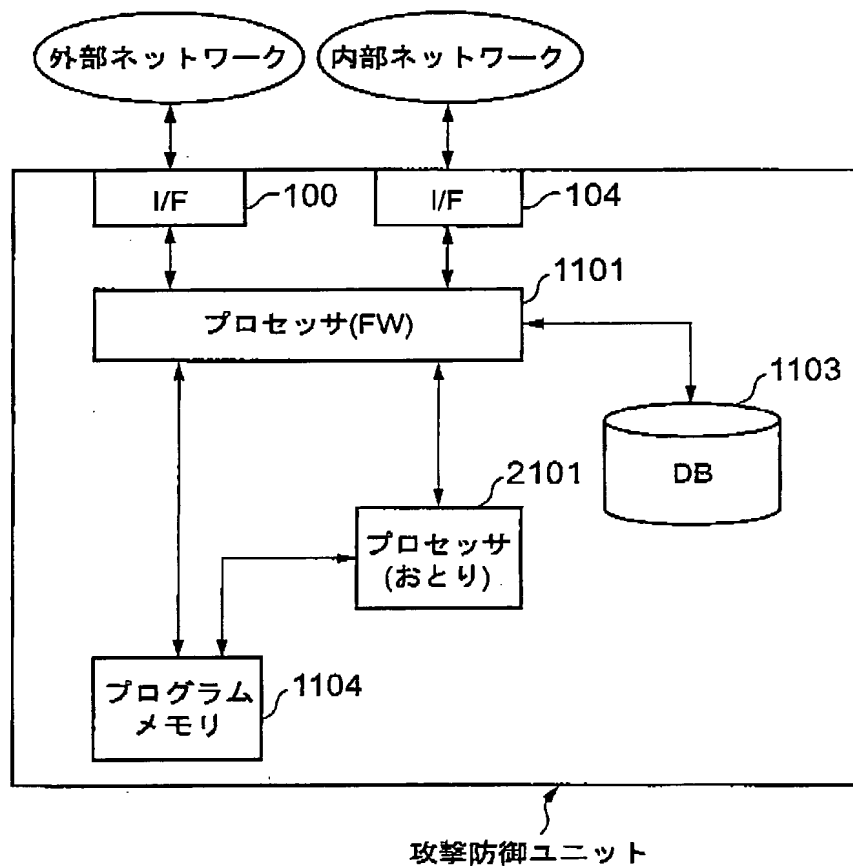


図33

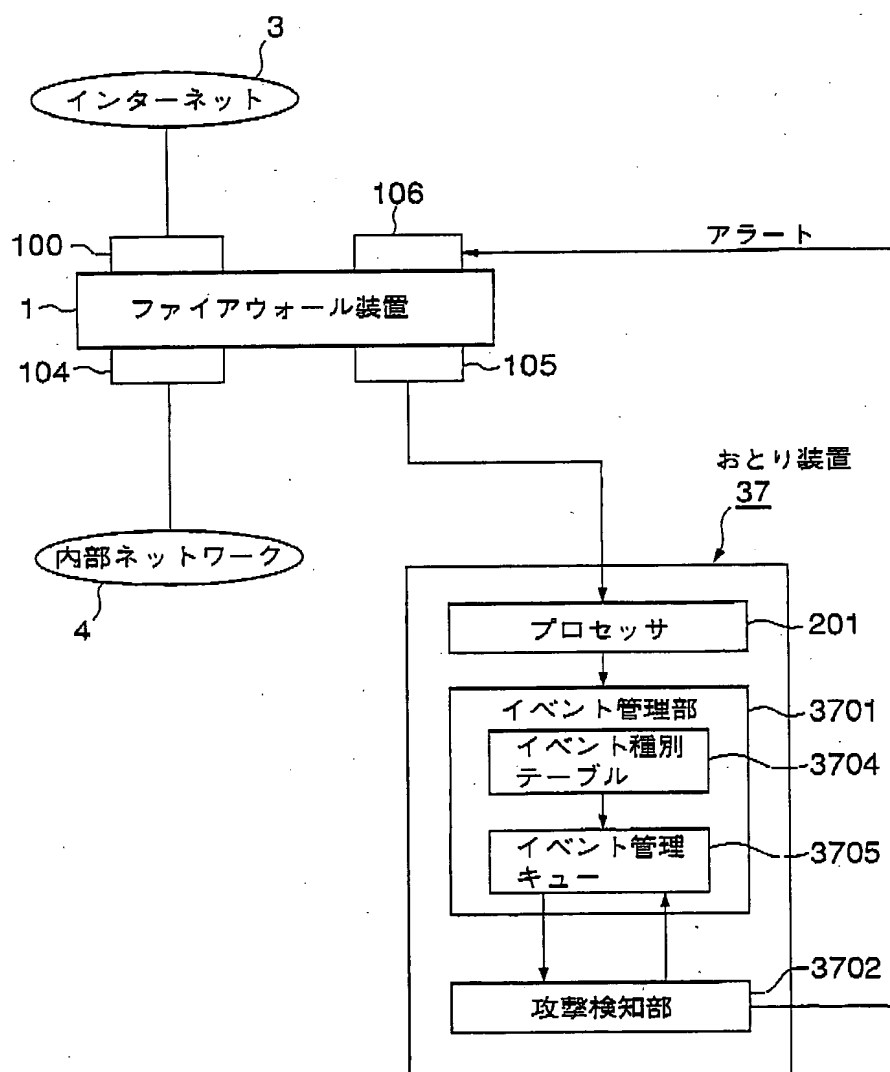




図34

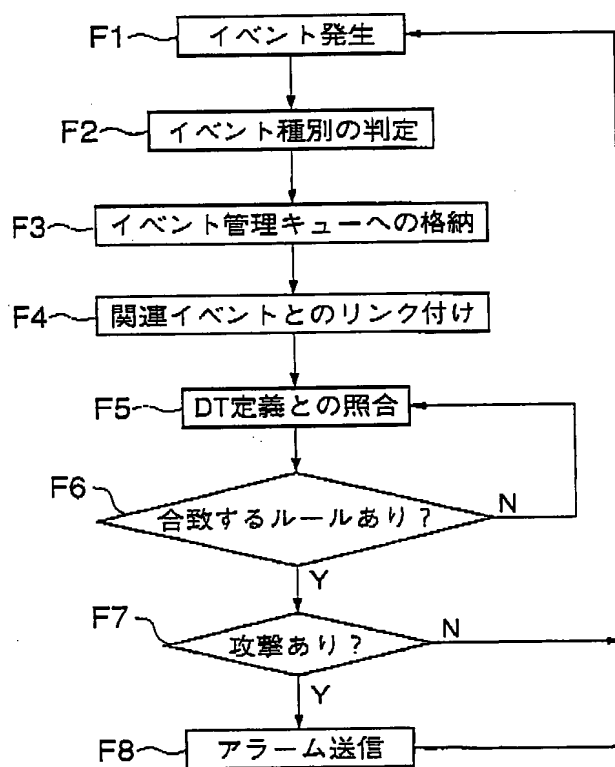




図37

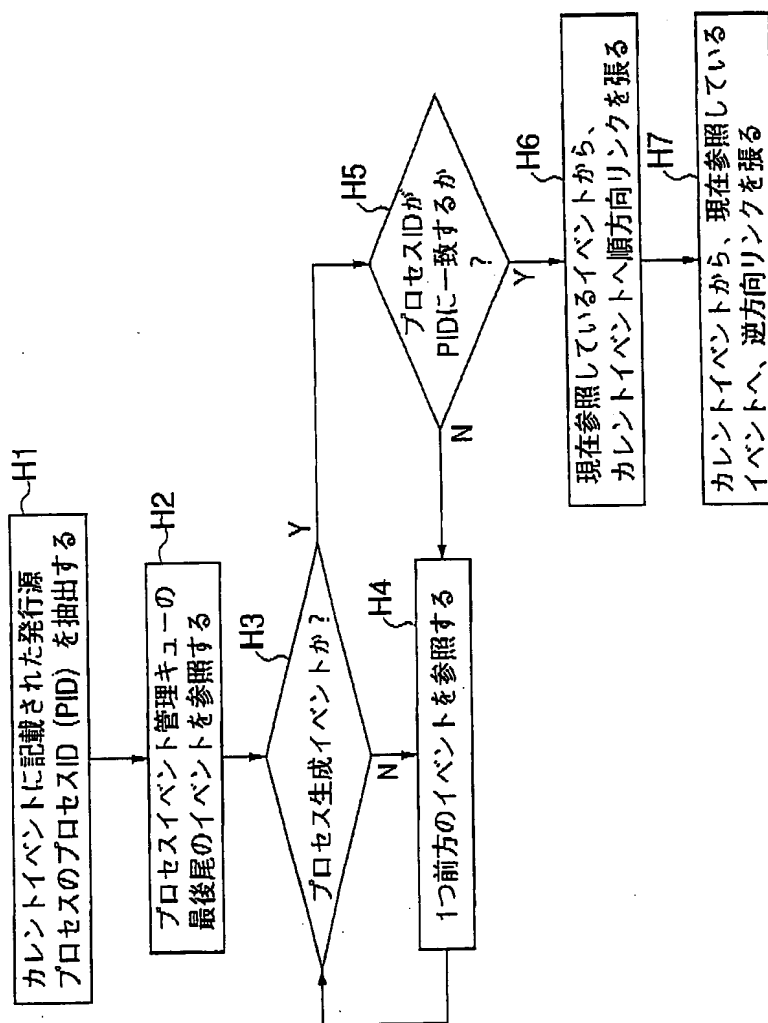


図38

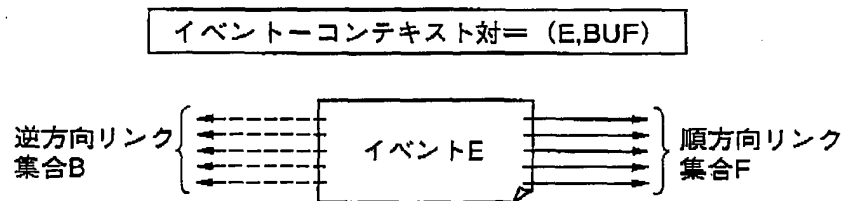


図39

## 4101 DT定義ファイル

```
# (ルール1) WWWサーバによるログの書き出しを許可する
0.0.0.0/0,<inetinfo.exe>,FILE_WRITE,C:%winnt%system32\LogFiles%.*;ALLOW
# (ルール2) WWWサーバによるコンテンツ領域の読み込みを許可する。
0.0.0.0/0,<inetinfo.exe>,FILE_READ,C:%inetpub%wwwroot%.*;ALLOW

# (ルール3) WWWサーバのサブシステムである登録CGIはデータベースを更新してよい。
0.0.0.0/0,<inetinfo.exe><regist.exe> $,FILE_WRITE,C:%data%client.db;ALLOW
# (ルール4) WWWサーバのサブシステムである出力CGIによるデータベース読み込みを許可。
0.0.0.0/0,<inetinfo.exe><view.exe> $,FILE_READ,C:%data%client.db;ALLOW

# (ルール5) FTPサーバはコンテンツ領域に書き出し可能
# ただし、管理者ドメイン10.56.192.0/24からのアクセスに限る
10.56.192.0/24.^<ftpd.exe>+ $,FILE_WRITE,C:%inetpub%wwwroot%.*;ALLOW

# (ルール6) WWWサーバは、特に許可されていない限り、ファイル書き出しを行わない。
0.0.0.0/0,<inetinfo.exe>,FILE_WRITE,.*;DENY
# (ルール7) 許可されたプログラム以外によるデータベース領域のアクセスを禁止する。
0.0.0.0/0,.*,FILE_READ;FILE_WRITE,C:%data%.*;DENY
# (ルール8) 許可されたプログラム以外によるコンテンツ領域の書換えは攻撃である。
0.0.0.0/0,.*,FILE_WRITE,C:%inetpub%wwwroot%.*;DENY

# (デフォルトルール) どのルールにもマッチしない場合は「許可」
DEFAULT;ALLOW
```

図40

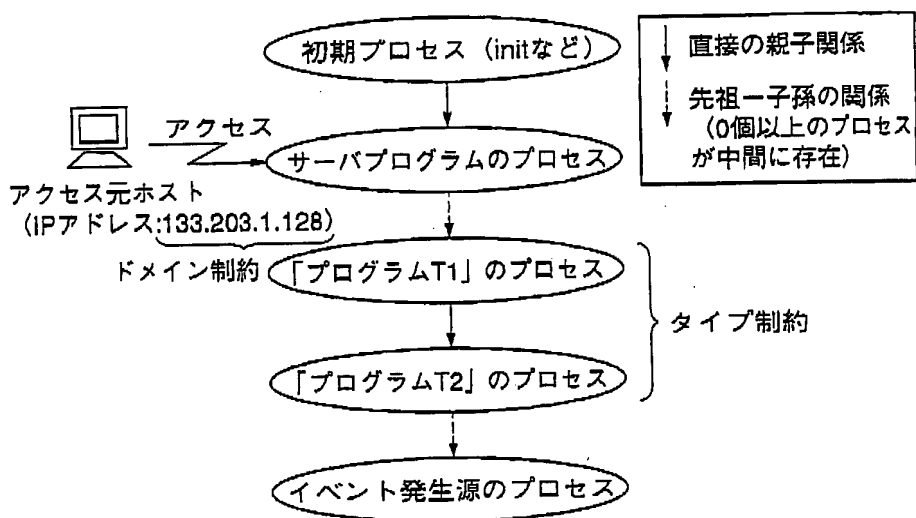


図41

3501

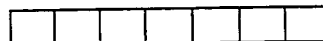
イベント名: NW\_ACCEPT  
パラメータ: ("src\_addr=133.207.57.2","src\_port=13485")  
返り値: "fd=15"  
発行プロセスID: 709

追加

ネットワークイベント管理キュー



プロセスイベント管理キュー



ファイルイベント管理キュー



00537

366

図42

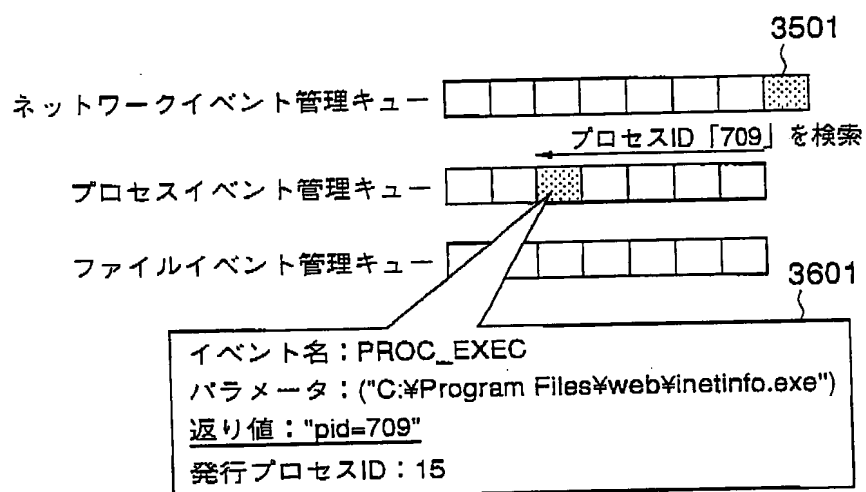
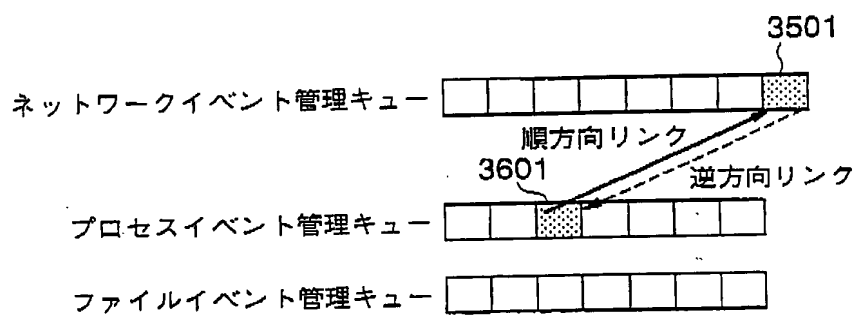


図43



00537

図44

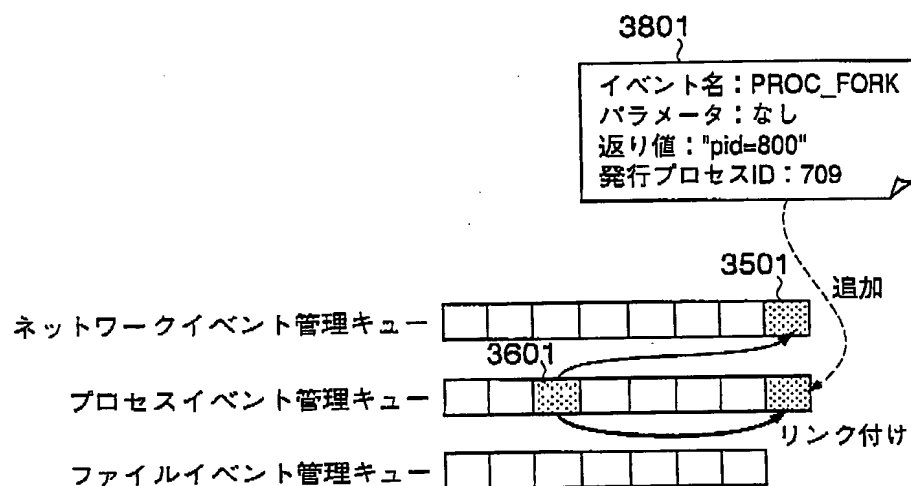


図45

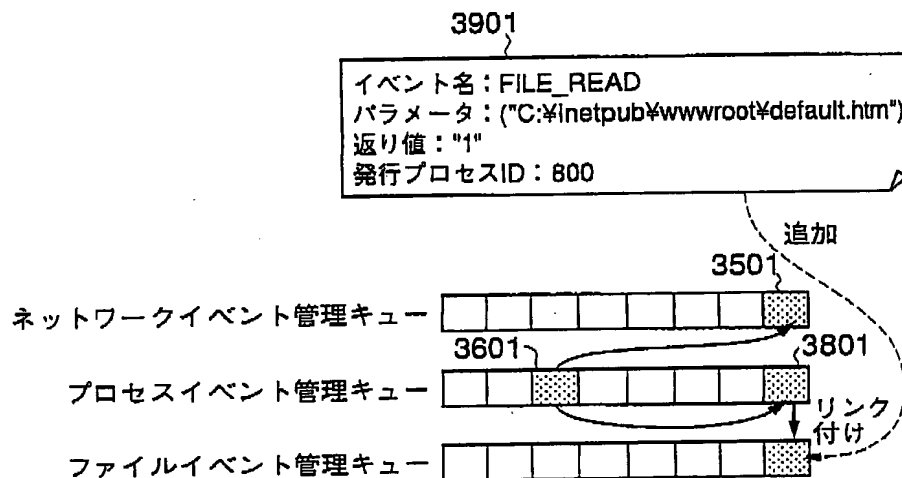


図46

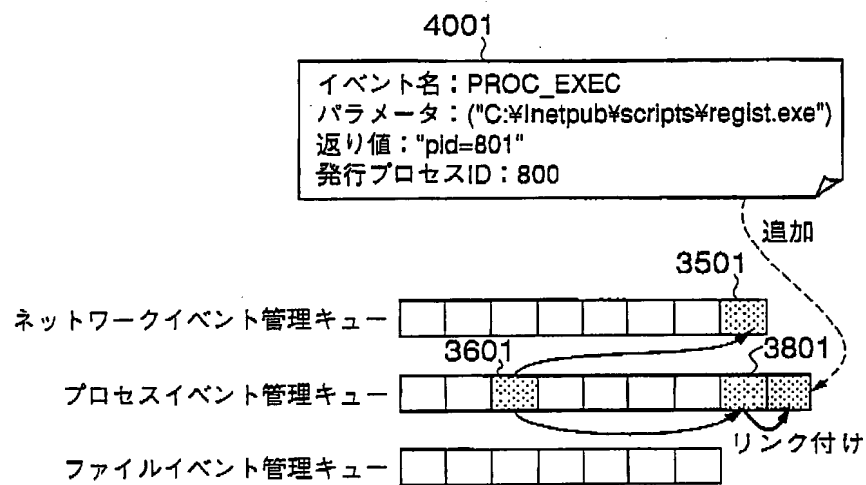
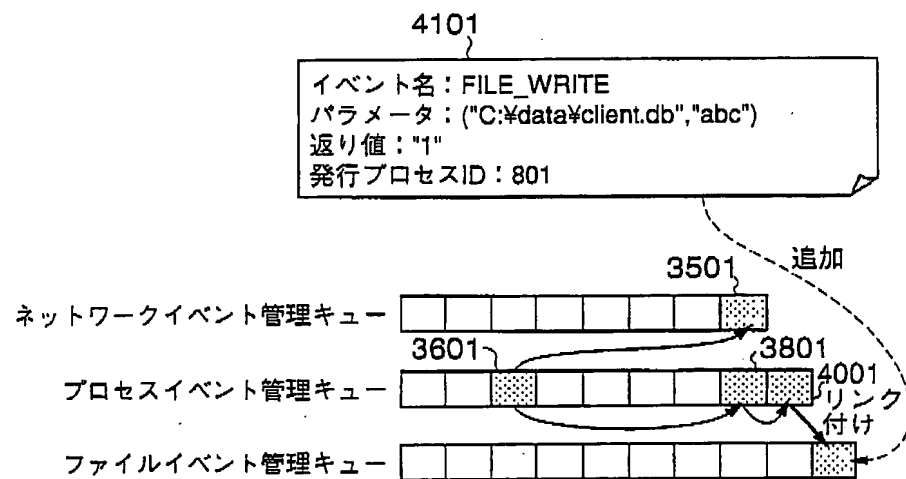


図47





00537

41

図48

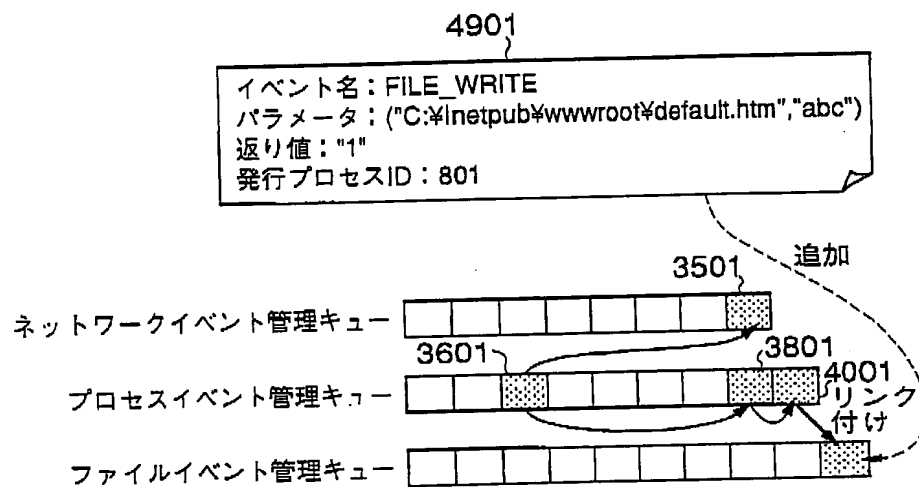


図49

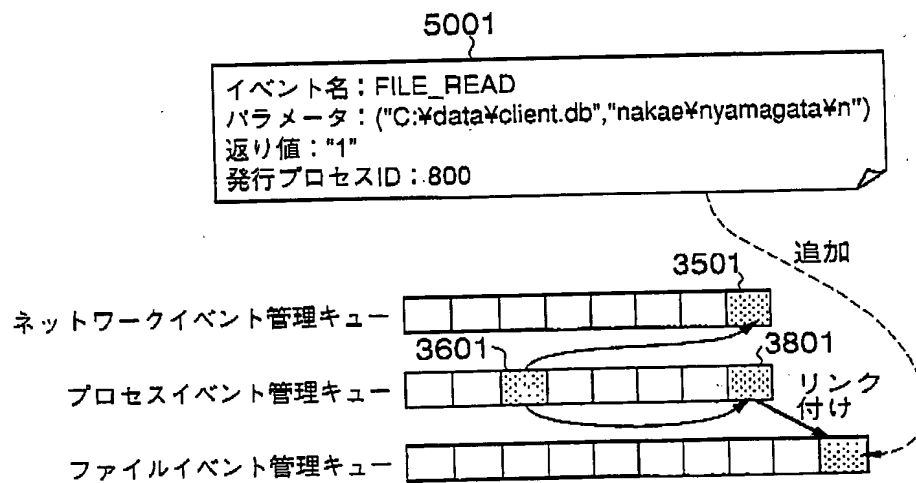


図50

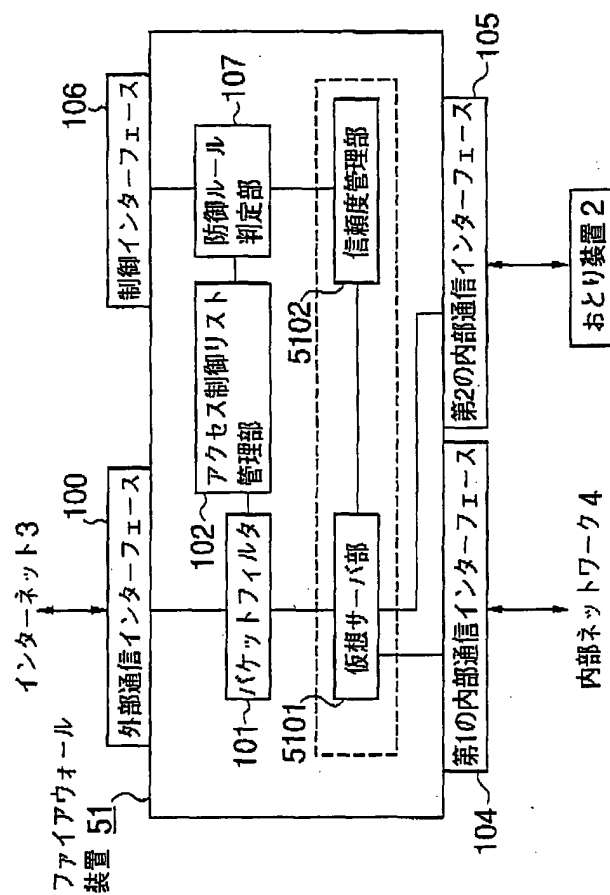
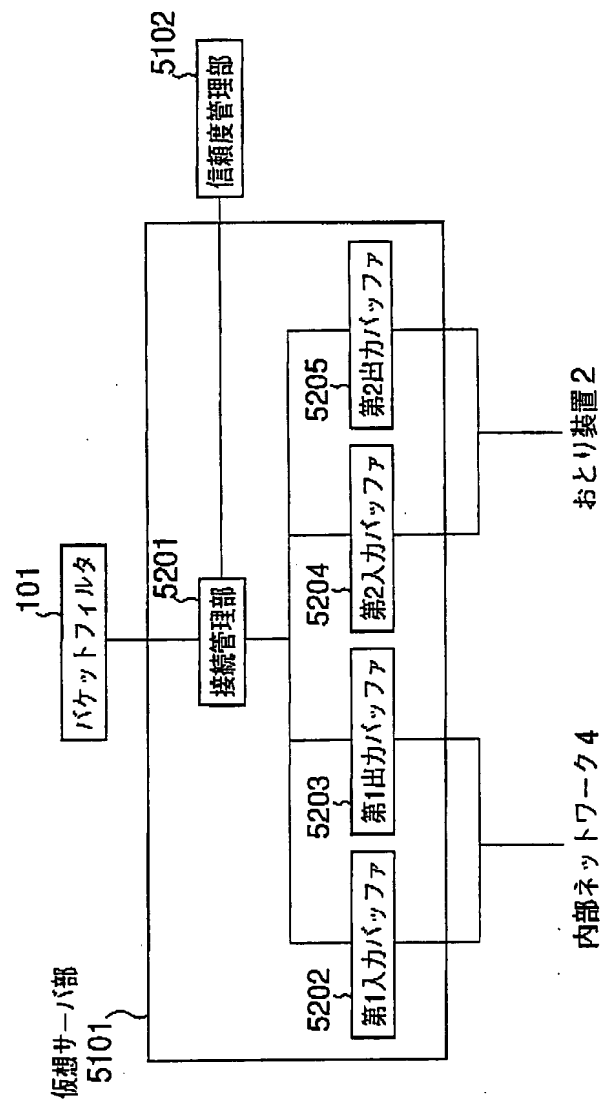
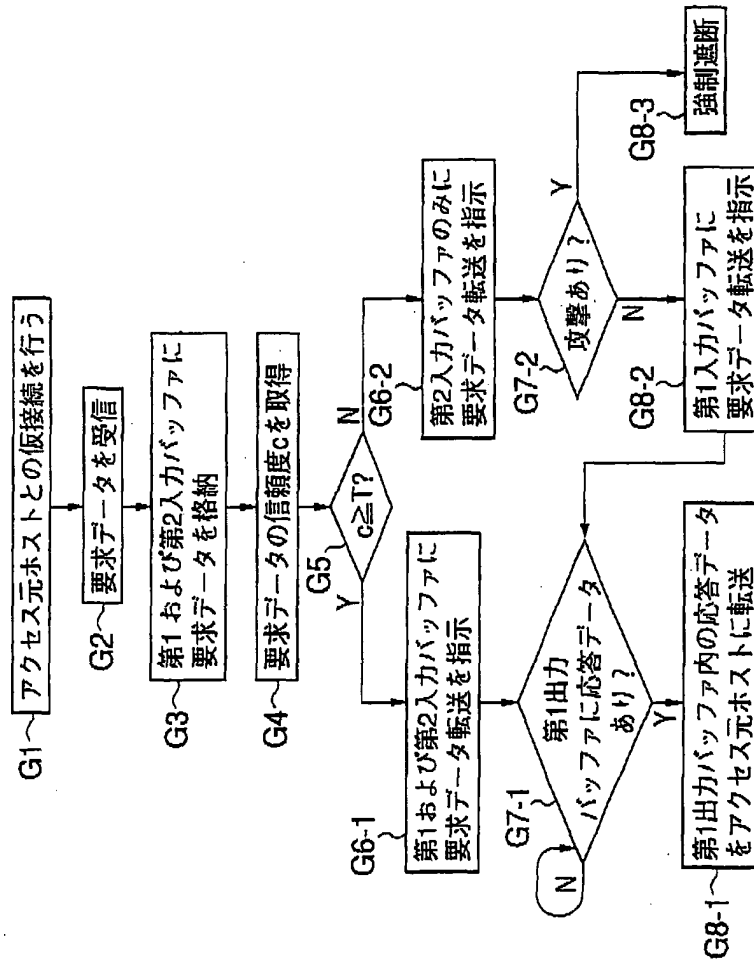


図51



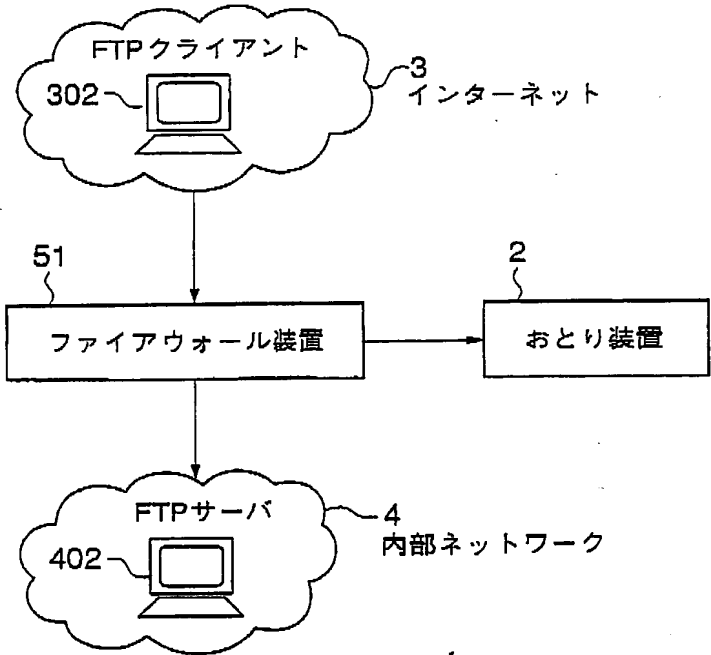


00537

図53

要求データ	信頼度
D0	1
D1	0
...	...
Dn	1

図54

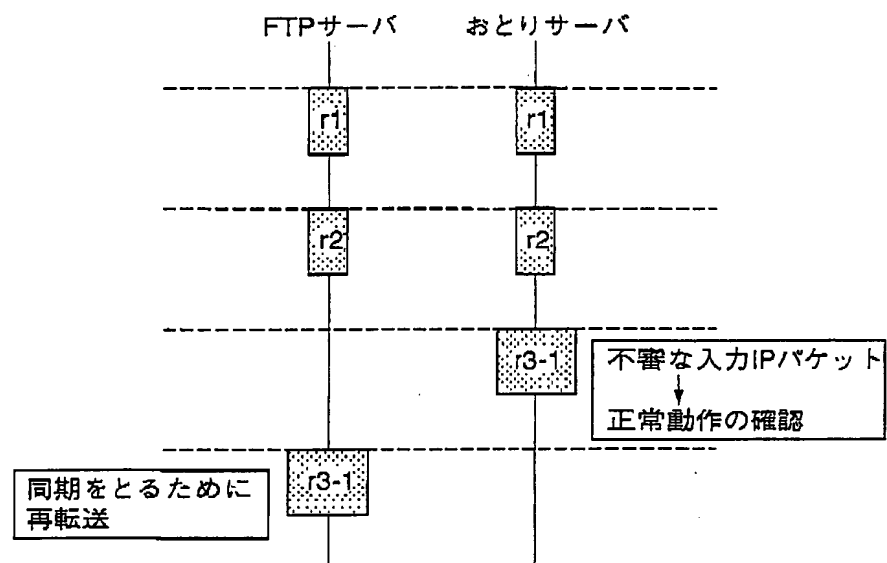


00537

図55

要求データ	信頼度
D0	1
D1	0
...	...
1	0

図56



00537

47

図57

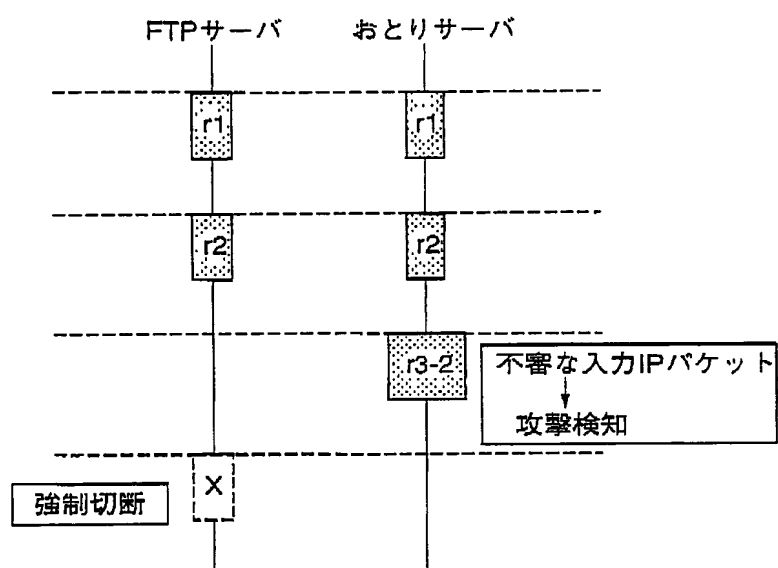
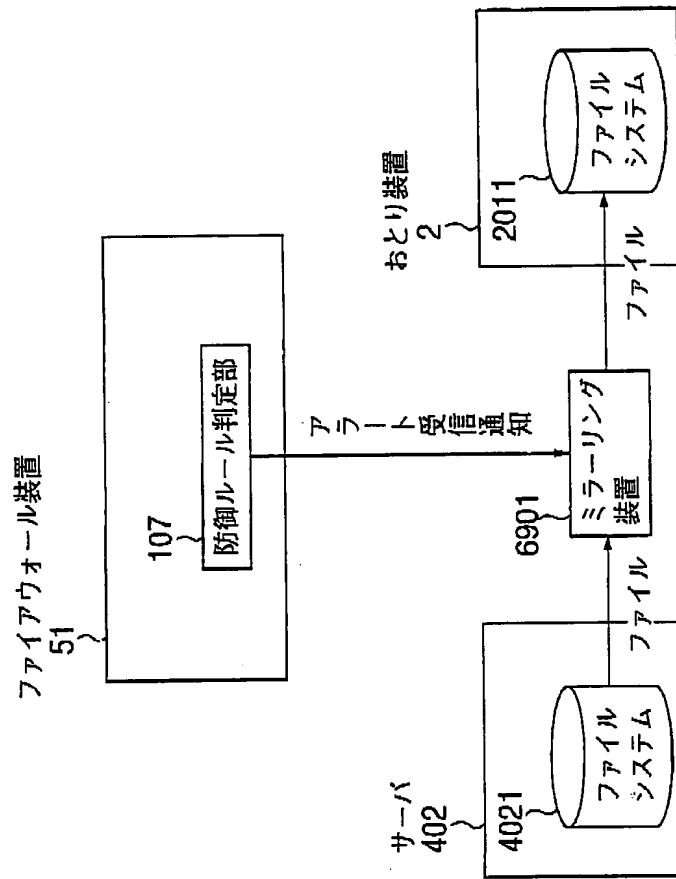


図58





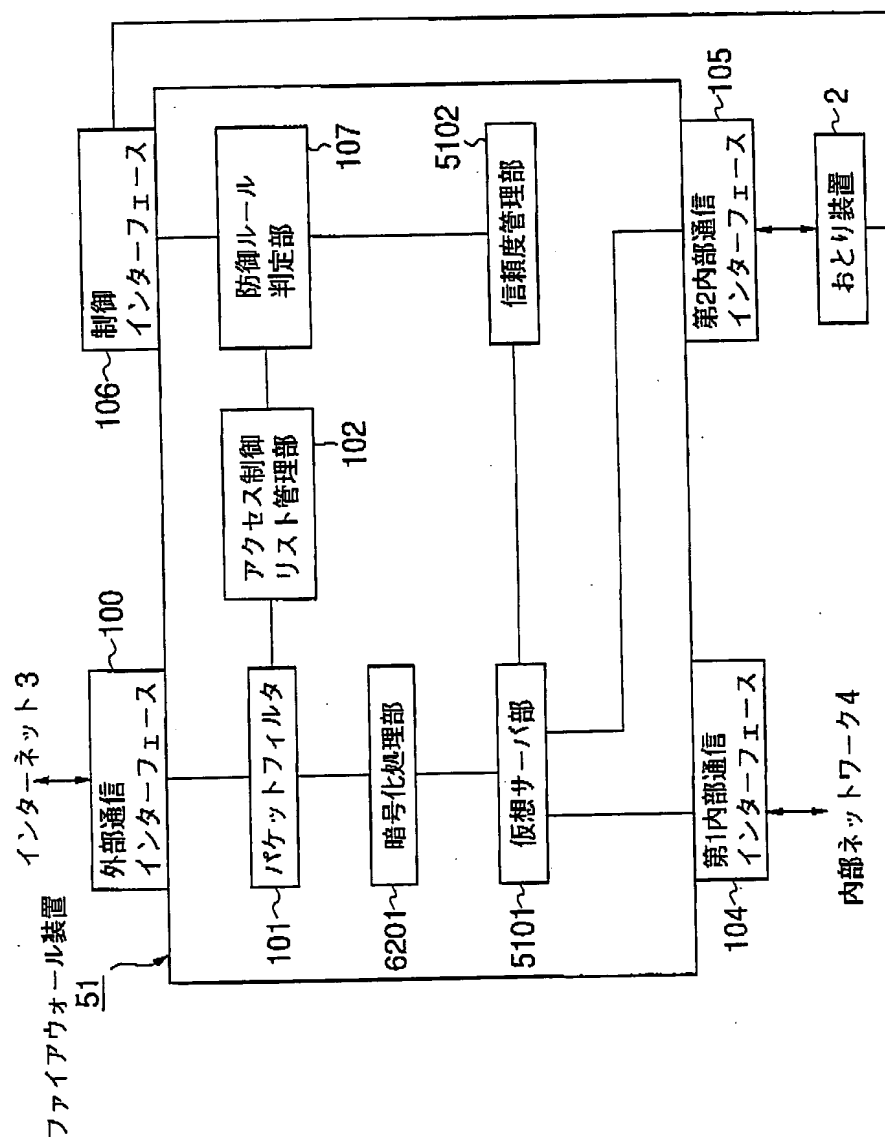
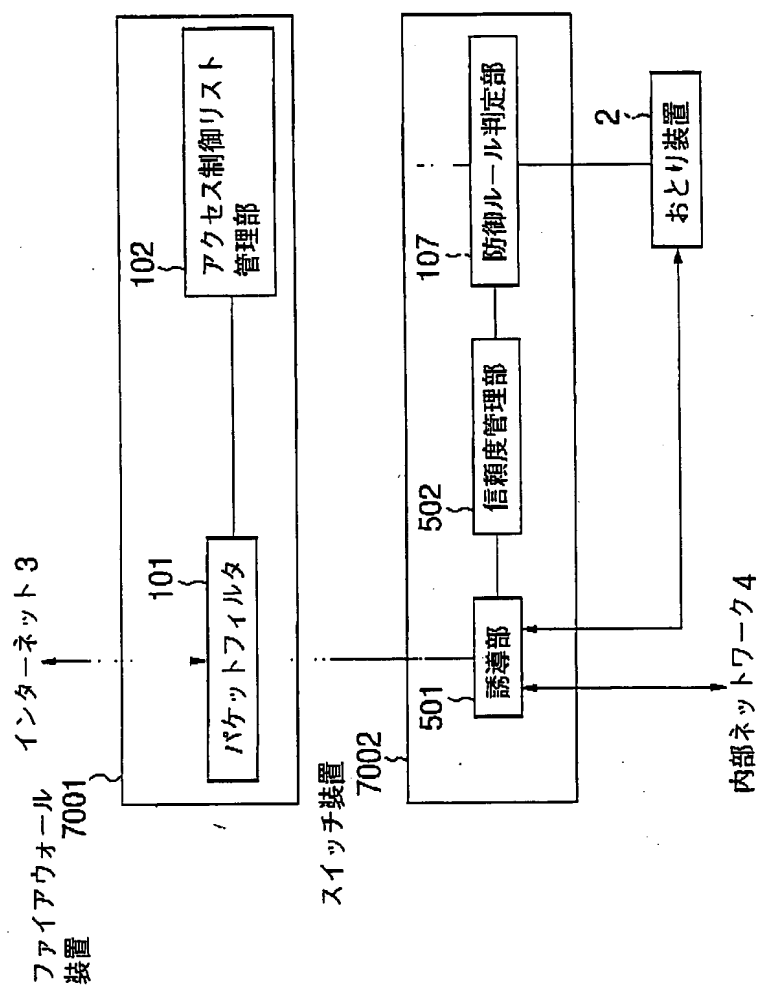


図60



00537

図61

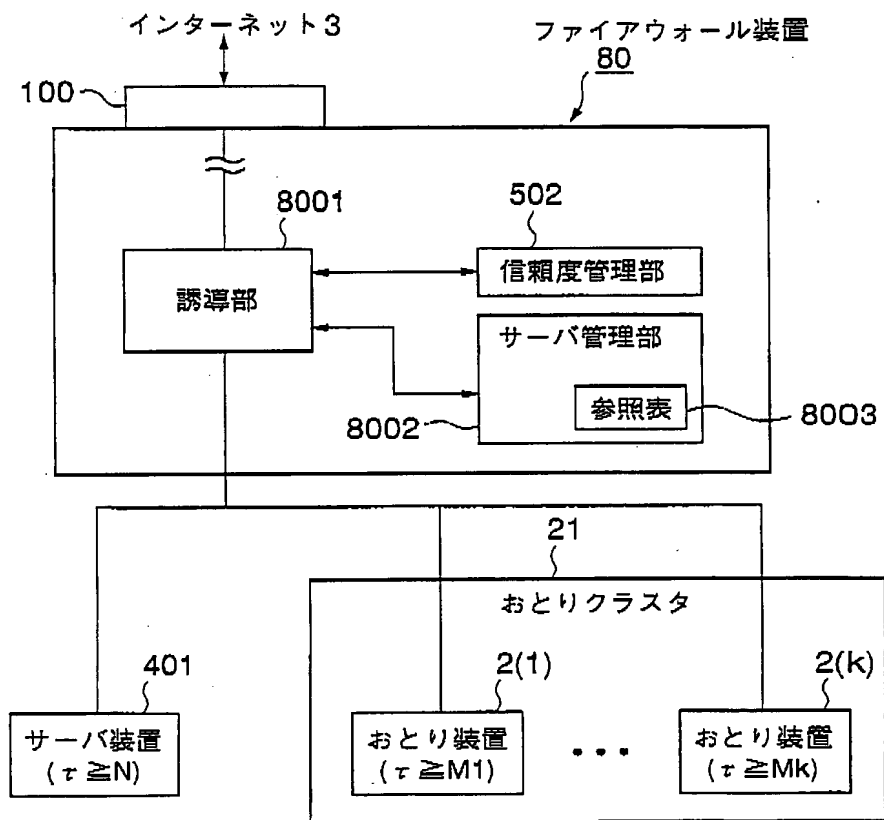


図62

8003 参照表

サーバ識別子	必須信頼度
D1	M1
D2	M2
...	...
Dk	Mk

図63

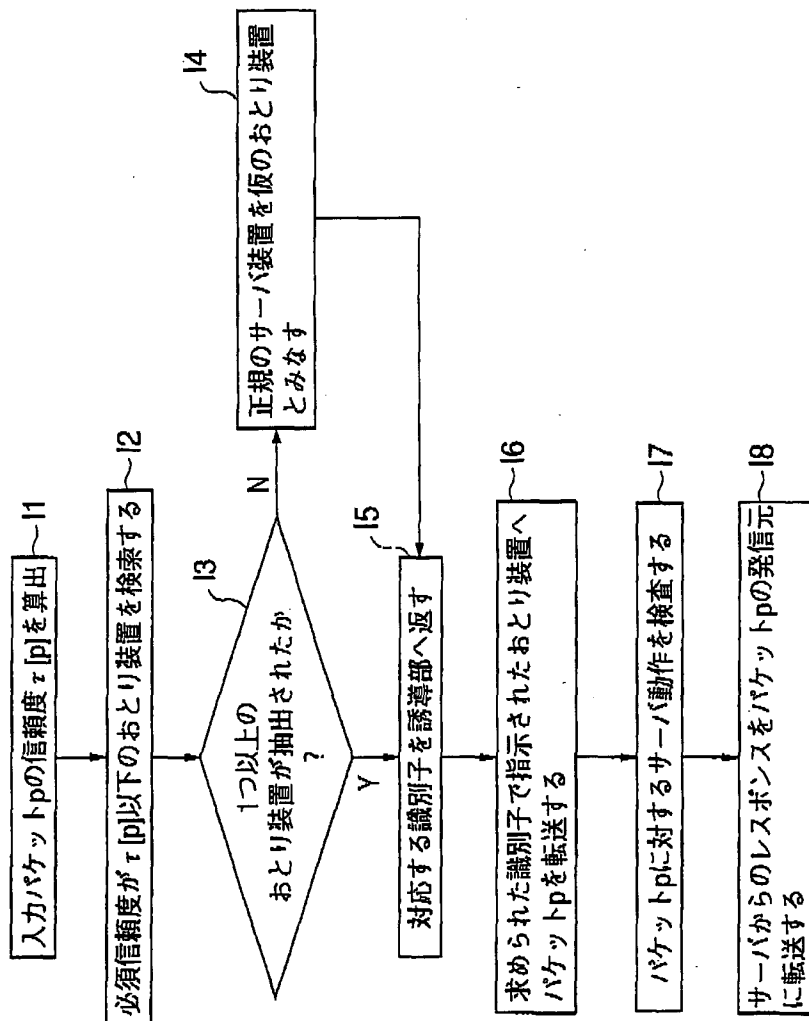
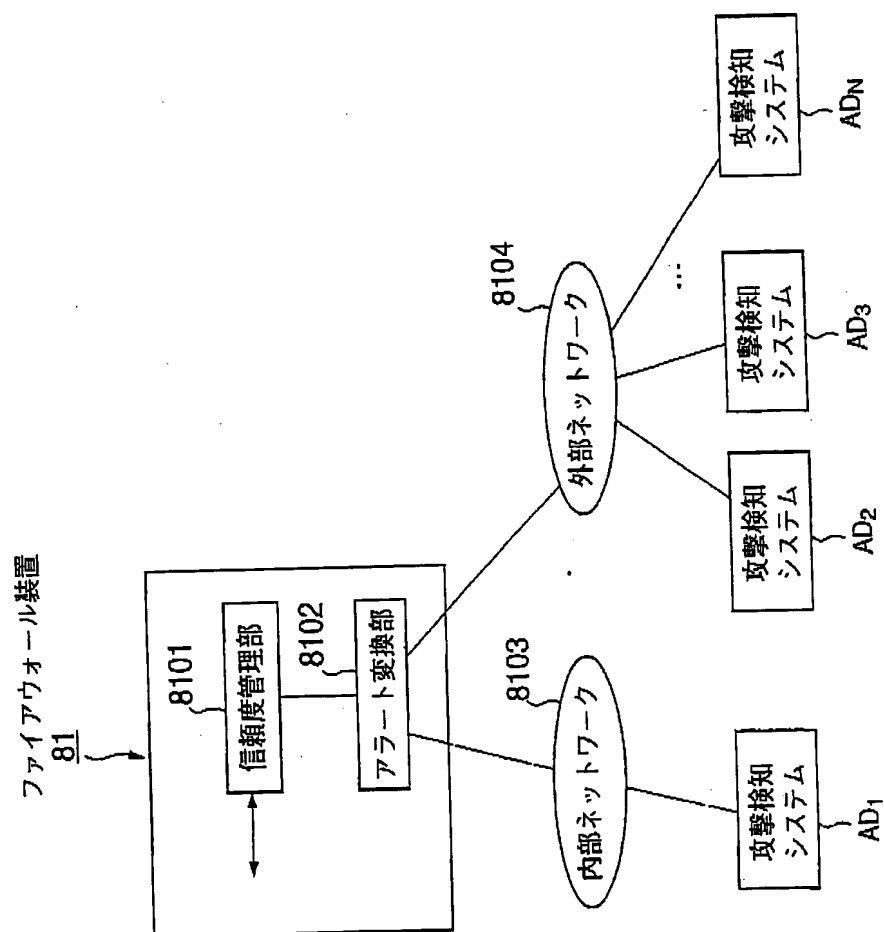


図64



00537

54

図65

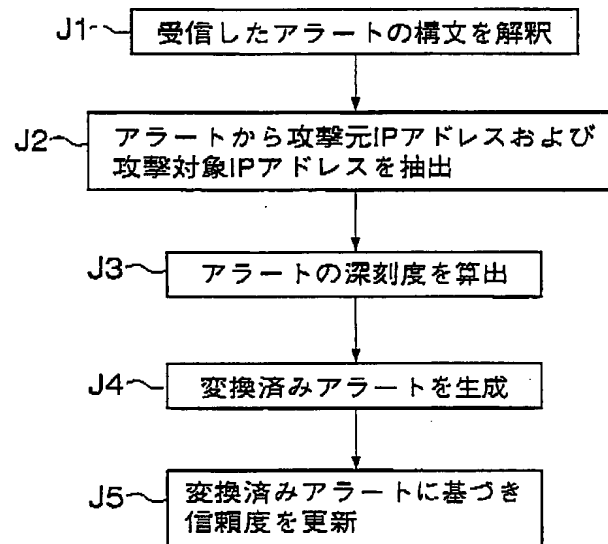


図66

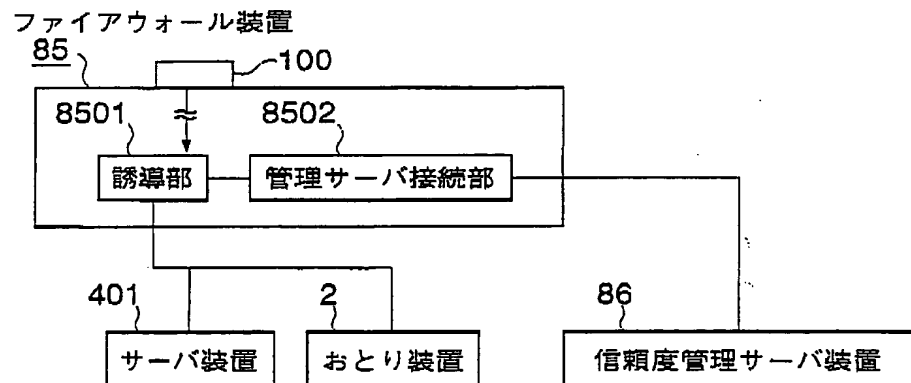


図67

